Expansive Automata Networks*

Florian Bridoux

Université Aix-Marseille, CNRS, LIS, Marseille, France

Maximilien Gadouleau

Department of Computer Science, Durham University, Durham, UK

Guillaume Theyssier*

Université Aix-Marseille, CNRS, I2M, Marseille, France

Abstract

An Automata Network is a map $f : Q^n \to Q^n$ where Q is a finite alphabet. It can be viewed as a network of n entities, each holding a state from Q, and evolving according to a deterministic synchronous update rule in such a way that each entity only depends on its neighbors in the network's graph, called interaction graph. In this work we introduce the following property called expansivity: the observation of the sequence of states at any given node is sufficient to determine the initial configuration of the whole network. A major trend in automata network theory is to understand how the interaction graph affects dynamical properties of f. Our first result is a characterization of interaction graphs that allow expansivity. Moreover, we show that this property is generic among linear automata networks over such graphs with large enough alphabet. We show however that the situation is more complex when the alphabet is fixed independently of the size of the interaction graph: no alphabet is sufficient to obtain expansivity on all admissible graphs, and only non-linear solutions exist in some cases. Besides, we show striking differences between the linear and the general non-linear case, in particular we prove that deciding expansivity is PSPACE-complete in the general case, while it can be done in polynomial time in the linear case. Finally, we consider a stronger version of expansivity where we ask to determine the initial configuration from any large enough observation of the system. We show that it can be achieved for any number of nodes and naturally gives rise to maximum distance separable codes.

Keywords: Automata networks, expansivity, MDS codes, PSPACE-completeness

*This work was partially funded by the CNRS and Royal Society joint research project PRC1861 and the French ANR project FANs ANR-18-CE40-0002.

*Corresponding author

1. Introduction

Networks of interacting entities can be modelled as follows. The network consists of n entities, where each entity v has a local state represented by a q-ary variable $x_v \in [\![q]\!] = \{0, 1, \dots, q-1\}$, which evolves according to a deterministic function $f_v : [\![q]\!]^n \to [\![q]\!]$ of all the local states. More concisely, the configuration of the network is $x = (x_1, \dots, x_n) \in [\![q]\!]^n$, which evolves according to a deterministic function $f = (f_1, \dots, f_n) : [\![q]\!]^n \to [\![q]\!]^n$. The function f, which encodes everything about the network, is referred to as an **Automata Network**, or simply network (the term Finite Dynamical Systems has also been applied for these networks). When speaking about properties of an automata network (like bijectivity), we mean a property of the function f. Automata networks have been used to model different networks, such as gene networks, neural networks, social networks, or network coding (see [1] and references therein for the applications of Automata networks). They can also be considered as a distributed computational model with various specialized definitions like in [2, 3]. The architecture of an Automata network $f : [\![q]\!]^n \to [\![q]\!]^n$ can be represented via its **interaction graph**, which indicates which update functions depend on which variables. In other words, the interaction graph represents the underlying network of entities and their influences on one another. A major topic of interest is to determine how the interaction graph affects different properties of the network, such as the number of fixed points or images (see [4] for a review of known results on the influence of the interaction graph). In particular, a stream of work aims to design networks with a prescribed interaction graph and with a specific dynamical property, such as a being bijective [5], or having many fixed points [6], or converging towards a fixed point [1].

In this paper, we introduce the concept of **expansive** networks. A network is expansive if the initial configuration of the network can be determined from the future temporal evolution of any local state. Formally, if f_v^t denotes the map $x \mapsto (f^t(x))_v$, f is expansive if it satisfies the equivalent conditions:

1. For any $v \in \{1, \dots, n\}$, there exists a natural number T such that the function $x \mapsto (f_v(x), \dots, f_v^T(x)) : [\![q]\!]^n \to [\![q]\!]^T$ is injective.

2. For any $v \in \{1, \dots, n\}$ and any distinct $x, y \in [\![q]\!]^n$, there exists $t \geq 1$ such that $f_v^t(x) \neq f_v^t(y)$.

We are mostly interested in general results on automata networks per se, without any particular application in mind. Nonetheless, as mentioned above, automata networks are versatile and can be seen and used from different points of view. The concept of expansive automata networks introduced here is meaningful for several of them.

Dynamical systems. The term 'expansive' is coined after the classical notion of dynamical system theory which corresponds to a strong form of topological unpredictability [7]. In the case of cellular automata [8], this topological notion

has a concrete interpretation in terms of traces: the orbit of the whole system can be deduced from its temporal trace on a limited spatial region (there is a similar notion in the field of symbolic dynamics [9]). The definition above follows the same idea and in fact there is a precise correspondence between expansivity in cellular automata and expansivity in automata networks (see section 2.2). Recall that a finite deterministic system has an eventually periodic behavior and one could naively object that they are therefore always "simple" dynamically. Of course, finite doesn't mean small and the period can be exponentially large in the size of the system, making the previous objection largely inoperative in practice. Beyond this matter of size, we stress that the definition of expansivity above does represent a form of unpredictability in the following sense: a partial knowledge of the initial configuration (the state of at least one node is not completely known) is never sufficient to determine the orbit observed at a node (for any node). Said differently, although perfectly deterministic by definition, the system always behaves non-deterministically as soon as there is some imprecision in the initial conditions.

Modeling tool and control theory. With the general point of view of modeling in mind, one is interested in making predictions on the future of a system from partial observations. In particular some components of the systems might be difficult or impossible to observe. Expansive automata network correspond to a favorable case where observing any single component for some time is sufficient. It is also interesting to relax the kind of observations allowed on the system, like in the stronger form of expansivity we consider in section 8. In the context of control theory, the well-established notion of *observability* (R. Kalmanin, 1960s) corresponds to systems whose internal state can be determined by the observation of its output (see e.g. [10, 11] for different settings which are relevant in computer science). In this context, one is interested in determining whether a given system is observable or not. Expansivity can be seen as a form of observability if we consider that the output of our system is the trace at some node. Control theory was largely developed for linear systems and observability is well-understood and easy to determine in this case. The situation is similar for expansivity in our setting (see sections 2 and 3). In the non-linear case, testing these properties is hard and hardness results on expansivity are actually hardness results for the problem of observability in automata networks (see section 7).

Orthogonal arrays and maximum distance separable code. In an expansive automata network, the orbit of any configuration contains a lot of redundancy because knowing T consecutive states of any given node is sufficient to reconstruct the complete orbit. Pushing this idea further we obtain a stronger form of expansivty in section 8 which yields orthogonal arrays of index unity or equivalently maximum distance separable codes (see [12, 13]). More precisely the set of orbits of a certain length is the code, and, in the linear case, it can be compactly represented by just giving the global map f of the automata network.

Distributed computation. An expansive automata network can be seen as a distributed protocol which solves the problem of giving the knowledge of the whole network's configuration to each of its entities, and that works for any

initial condition of the system. Moreover, if the constant T in Property 1 above is optimal, *i.e.* equal to n, then the automata network has another interesting algorithmic property: initial configurations (n states) are mapped bijectively to sequences of states of length n at each node. Said differently, it gives a protocol to transform a random initial configuration to a temporal random sequence of states at each node (with the uniform distribution in both cases). Such expansive networks with optimal constant T exist as we show below.

Our main contributions. First, in section 3, we study the existence of expansive networks depending on the interaction graph. We characterize the graphs that admit an expansive network over some alphabet (Theorem 3.7): those are the graphs that are strongly connected (there is a path from any vertex to any other vertex) and coverable (the vertices can be covered by disjoint cycles). We show in particular that for such graphs, almost all linear networks over sufficiently large fields are expansive (Corollary 3.12). Second, in section 4, we focus on the non-existence of expansive networks over small alphabets. We show that for any fixed alphabet size q, there exist strongly connected and coverable graphs that do not admit any expansive network over $[\![q]\!]$ (Theorem 4.1). We also exhibit a graph which admits an expansive network over all alphabets, but does not admit any linear expansive network for an infinite number of alphabet values (Proposition 4.4). Then, in section 5, we focus on the minimum time $T(f)$, referred to as the expansion time, for which any difference between distinct configurations has been witnessed on all vertices. We notably prove that the expansion time can vary from n to almost q^n, and that the minimum of n is achieved by linear networks over fields (Theorem 5.4). In section 6, we consider the average number of differences between two orbits, called expansion frequency. We show that it can be arbitrarily close to 1 (Theorem 6.1) while previous section gave a construction showing that it can be arbitrarily close to 0. In section 7, we consider the decision problem of whether a given network is expansive. We prove that it is a PSPACE-complete problem (Theorem 7.7). Finally, in section 8, we consider a stronger notion of expansivity which asks to recover the initial configuration from any large enough observation of the system (not only the trace at a given node). We show that automata networks with that property yield maximum distance separable codes (Proposition 8.3) and exist on any complete interaction graph (Theorem 8.2), while they require an alphabet quadratic in the number of nodes (Corollary 8.4).

2. Definitions and preliminary results

Graphs. A (directed) graph is a pair $D = (V, E)$, where $E \subseteq V^2$. For concepts about graphs, the reader is referred to the authoritative book [14]. Let us simply highlight some concepts and their notation in this paper. For any graph $D = (V, E)$ and any set of vertices $S \subseteq V$, we denote the out-neighbourhood of S as $N_{\text{out}}(S) = \{u \in V : \exists s \in S \text{ s.t. } su \in E\}$; the in-neighbourhood is defined similarly and is denoted as $N_{\text{in}}(S)$. An arc of the form uu for some $u \in V$ is called a loop. A graph is loop-full if there is a loop on each vertex. For any

two vertices $u, v \in V$, the distance from u to v in D is the length of a shortest path from u to v in D; it is denoted as $d_D(u, v)$. The adjacency matrix of D, denoted A_D is the $n \times n$ matrix A_D with $A_D(i, j) = 1$ if $ij \in E$ and $A_D(i, j) = 0$ otherwise.

Automata networks. Let n be a positive integer and q be an integer no less than 2. We denote $[n] = \{1, \dots, n\}$ and $[\![q]\!] = \{0, \dots, q-1\}$. In the sequel n will always denote the size of the network and $[\![q]\!]$ its alphabet. A state is any element $x = (x_1, \dots, x_n) \in [\![q]\!]^n$. For any $S = \{s_1, \dots, s_k\} \subseteq [n]$, we denote $x_S = (x_{s_1}, \dots, x_{s_k})$; the order in which these indices occur will not matter usually. We denote the set of functions $f : [\![q]\!]^n \to [\![q]\!]^n$ as $\mathrm{F}(n, q)$. A network is any element of $\mathrm{F}(n, q)$. We can view f as $f = (f_1, \dots, f_n)$, where each f_v is a function $[\![q]\!]^n \to [\![q]\!]$. We can then use the same shorthand notation as for states, and define f_S for instance. We also often use the notation $f_v^t = (f^t)_v$. The interaction graph of $f \in \mathrm{F}(n, q)$ has vertex set $V = [n]$ and has an arc from u to v if and only if f_v depends essentially on u, i.e. there exists $a, b \in [\![q]\!]^n$ such that $a_{[n]\setminus u} = b_{[n]\setminus u}$ and $f_v(a) \neq f_v(b)$. If the interaction graph of f is D, we then say that D admits f. For any digraph D with n nodes, we denote the set of networks in $\mathrm{F}(n, q)$ with interaction graph D as $\mathrm{F}[D, q]$.

Linear networks. To obtain some results, we shall focus on networks of a special kind that can be analyzed through classical algebra; we give them in decreasing order of generality. A network is **abelian** if $[\![q]\!]$ is endowed with the structure of a finite abelian group A and f is an endomorphism of the group A^n. More concretely, we have $f_v(x) = \sum_{j \in [n]} e_{v,j}(x_j)$, where the $e_{v,j}$ are endomorphisms of A. A network is **linear** if $[\![q]\!]$ is endowed with a ring structure R and f is defined by some matrix M as $f(x) = xM$, where $M \in R^{n \times n}$. A network is **field linear** if it is linear over the finite field $\mathrm{GF}(q)$ of order q. The **XOR network** on D is $f \in \mathrm{F}[D, 2]$, defined by $f(x) = xA_D$, where A_D is the adjacency matrix of D. This is the only abelian network with interaction graph D for $q = 2$. Note that from the perspective of both positive expansivity in cellular automata and control theory, the restriction to linear (or even abelian) system is common in the literature.

2.1. Trace and expansive networks

Fix $f \in \mathrm{F}(n, q)$. Then for any x and v, the **trace** of x at v is the infinite (ultimately periodic) sequence $\rho_v(x) = (f_v(x), f_v^2(x), \dots)$. We also denote $\rho_v^{(T)}(x) = (f_v(x), \dots, f_v^T(x))$ as the first T elements in the trace.

Definition 2.1. *A network f is **expansive** if for any distinct $x, y \in [\![q]\!]^n$ and any $v \in [n]$, there exists $t \geq 1$ such that $f_v^t(x) \neq f_v^t(y)$. Equivalently, f is expansive if and only if for any v, there exists $T \geq 1$ such that the trace function $\rho_v^{(T)}$ is injective.*

When f is abelian, the function $(f_v, f_v^2, \dots, f_v^T) : [\![q]\!]^n \to [\![q]\!]^T$ is also abelian. Therefore, if f is abelian then f is expansive if and only if for all $x \in [\![q]\!]^n \setminus$

$\{(0,\ldots,0)\}$ and all $v \in [n]$, there exists $t \geq 1$ such that $f_v^t(x) \neq f_v^t(0,\ldots,0)$. Let f be a linear network, i.e. $f(x) = xM$. From M, construct the powers of M: $M^0 = I, M^1 = M, M^2, \ldots$; denote the u-th column of M^i as M_u^i. For any $t \geq 0$ and any $u \in [n]$, construct the matrix

$$N_u^{(t)} = \left(\begin{array}{c|c|c|c} M_u^t & M_u^{t+1} & \ldots & M_u^{t+n-1} \end{array} \right).$$

The matrices $N_u^{(t)}$ then determine whether f is expansive when f is field linear.

Lemma 2.2. *The following are equivalent for a field linear network $f(x) = xM$.*

1. *f is expansive.*
2. *M is nonsingular and $N_u^{(0)}$ is nonsingular for all $u \in [n]$.*
3. *$N_u^{(t)}$ is nonsingular for all $u \in [n]$ and $t \geq 1$.*
4. *There exists $t \geq 1$ such that $N_u^{(t)}$ is nonsigular for all $u \in [n]$.*

Proof. We prove 2 implies 3. Since $M_u^{t+k} = M^t M_u^k$, we have $N_u^{(t)} = M^t N_u^{(0)}$. Thus, if M and $N_u^{(0)}$ are nonsingular, then so is $N_u^{(t)}$. Clearly, 3 implies 4. We prove 4 implies 1. Suppose 4 holds, and let $y = (f_u^t(x), \ldots, f_u^{t+n-1}(x)) = xN_u^{(t)}$. Then $x = y(N_u^{(t)})^{-1}$ can be recovered from y and f is expansive. We prove 1 implies 2. Clearly, if f is expansive, then it is bijective, thus M is nonsingular. Suppose that f is expansive, but $N_u^{(0)}$ is singular for some u. By expansivity, there exists $s > n$ such that the matrix

$$\tilde{N}_u^{(s)} = \left(\begin{array}{c|c|c|c} M_u^0 & M_u^1 & \ldots & M_u^{s-1} \end{array} \right)$$

has full rank (*i.e.* rank n). However, because $N_u^{(0)} = \tilde{N}_u^{(n)}$ is singular, there exists $j < n$ such that M_u^j is in the column span of $\tilde{N}_u^{(j)}$. Say $M_u^j = \sum_{i=0}^{j-1} y_i M_u^i$, then we have for all $k \geq 0$

$$M_u^{j+k} = M^k M_u^j = M^k \sum_{i=0}^{j-1} y_i M_u^i = \sum_{i=0}^{j-1} y_i M_u^{i+k}.$$

Thus, $\mathrm{rk}(\tilde{N}_u^{(s)}) = \mathrm{rk}(\tilde{N}_u^{(j)}) \leq \mathrm{rk}(N_u^{(0)}) < n$, which is the desired contradiction. □

Since computing the determinant is no harder than multiplying matrices [15, Theorem 6.6], Property 2 yields an efficient algorithm to determine the expansivity of a field linear network.

Corollary 2.3. *Determining whether a field linear network is expansive can be done in $\mathcal{O}(n \cdot M(n))$, where $M(n)$ is the running time of an $n \times n$ matrix multiplication algorithm.*

2.2. Links with expansivity in cellular automata

A topological dynamical system [8] is a pair (F, X) where X is a compact metric space with distance d and F a continuous map. F is said positively expansive if there is a real constant $\epsilon > 0$ such that:

$$\forall x, y \in X : x \neq y \Rightarrow \exists t \geq 0, d(F^t(x), F^t(y) \geq \epsilon.$$

Note that the original setting in [7] assumes that F is bijective and defines the weaker notion of expansivity where t might be chosen negative.

A (one-dimensional) cellular automaton is a topological dynamical system $(F, Q^{\mathbb{Z}})$ where Q is a finite alphabet and F is defined through a local rule $f : Q^V \to Q$ with $V = [-r, \dots, r]$ called neighborhood as follows:

$$\forall x \in Q^{\mathbb{Z}}, \forall z \in \mathbb{Z}, F(x)_z = f(x_{|z+V})$$

where $x_{|z+V}$ denotes the map: $i \in V \mapsto x_{z+i}$. F is positively expansive if and only if the following trace map is bijective [8, Proposition 5.48]:

$$x \mapsto (x_{|V}, F(x)_{|V}, F^2(x)_{|V}, \dots)$$

or equivalently if and only if

$$\forall x, y \in X, x \neq y \Rightarrow \exists t : F^t(x)_{|V} \neq F^t(y)_{|V}.$$

Expansivity (positive or not) in cellular automata has received a lot of attention [16, 17, 18] and is still an active direction of research [19], one of the main open problem being the decidability of the property (see [20, Problem 19] or [21, Problem 7]).

The link between expansive cellular automata and automata networks can be made more explicit through the notion of quasi-expansivity.

Definition 2.4. *A network f is **quasi-expansive** if for all $x \neq y$ and all v, there exists $t \geq 0$ such that $f^t_{N_{\text{in}}(v)}(x) \neq f^t_{N_{\text{in}}(v)}(y)$.*

Note that the main notion of expansivity of the current paper (definition 2.1) is stronger than quasi-expansivity. We can then establish a correspondence between cellular automata and automata networks in two ways (to simplify exposition and stick exactly to the definition of dependency graph we suppose that the local map $f : Q^V \to Q$ essentially depends on all its variables):

1. we can see a cellular automaton F as an automata network on the infinite graph $(\mathbb{Z}, E)$ where $(i, j) \in E$ if and only if $|i - j| \leq r$ (taking the notation above). Note that this graph is always strongly connected and can be covered by disjoint cycles (see Theorem 3.7) and F as a cellular automaton is positively expansive if and only if it is quasi-expansive as an (infinite) automata network. In particular expansivity of F as an automata network implies positive expansivity of F as a cellular automaton.

2. we can also restrict a cellular automaton F to periodic configurations of period n. In this case it can be seen as a standard automata network F_n on the finite graph $(\mathbb{Z}/n\mathbb{Z}, E)$ where $(i, j) \in E$ if and only if $|i - j| \leq r$. If F as a cellular automaton is positively expansive, then for any n, the automata network F_n is quasi-expansive. The converse is false as the shift cellular automaton $F(x)_z = x_{z+1}$ is not positively expansive while all its restrictions F_n are quasi-expansive.

3. Interaction graphs of expansive networks

In this section, we are interested in determining for which interaction graphs D there exists an expansive network in $\mathrm{F}[D, q]$. Some graphs admit expansive network for any alphabet (subsection 3.2), some admit no expansive network whatever the alphabet. The main result of this section is a characterization of graphs admitting an expansive network for some alphabet (subsection 3.3).

3.1. Bijective networks

Since an expansive network is bijective, we first derive a result about the existence of bijective networks. A cycle decomposition of a graph D is a set of vertex-disjoint cycles that partition the vertex set of D. Say a graph D is **coverable** if it has a cycle decomposition. A digraph is coverable if and only if $|N_{\mathrm{out}}(S)| \geq |S|$ for all $S \subseteq V$ [14, Proposition 3.11.6]. These graphs can be characterized through existence of bijective networks.

Theorem 3.1 ([5])**.** *D is coverable if and only if $\mathrm{F}[D, q]$ contains a bijection for all $q \geq 3$.*

We first give a similar result on bijections in the linear case. Let $\mathrm{M}[D, q]$ denote the set of matrices over $\mathbb{Z}_q$ and with interaction graph equal to D, *i.e.* matrices M such that: $M_{i,j} \neq 0 \iff ij \in E(D)$.

Theorem 3.2. *If D is coverable, then $\mathrm{M}[D, q]$ contains a nonsingular matrix for any $q \geq 3$.*

Proof. Let us first settle the case where D is loop-full. We shall prove that there exists a matrix $M \in \mathrm{M}[D, q]$ with determinant equal to 1. The result is clear for $n = 1$, so suppose it holds for $n - 1$. Let $M' \in \mathrm{M}[D \setminus n, q]$ have determinant 1. Then let $A \in \mathrm{M}[D, q]$ such that

$$A_{i,j} = \begin{cases} M'_{i,j} & \text{if } i, j \neq n \\ 1 & \text{if } i = n \text{ and } j \neq n \text{ and } ij \in E, \text{or if } i \neq n \text{ and } j = n \text{ and } ij \in E, \\ 1 & \text{if } i = j = n \\ 0 & \text{otherwise,} \end{cases}$$

If $\det(A) \neq 2$, then consider $M \in \mathrm{M}[D, q]$ such that

$$M_{i,j} = \begin{cases} 2 - \det(A) & \text{if } i = j = n, \\ A_{i,j} & \text{otherwise.} \end{cases}$$

Then $\det(M) = \det(A) + (M_{n,n} - 1)\det(M') = 1$. If $\det(A) = 2$, then let $M \in \mathrm{M}[D, q]$ such that

$$M_{i,j} = \begin{cases} 2 & \text{if } i = j = n, \\ -A_{i,j} & \text{if } j = n, i \neq n, \\ A_{i,j} & \text{otherwise.} \end{cases}$$

We then have $\det(M) = \det(A) - \det(M') = 1$ which shows the induction step for n and settles the case where D is loop-full.

In the general case, let D be coverable, then the mapping $v \mapsto \pi(v)$, where $\pi(v)$ is the successor of v on a cycle in the cycle partition is a permutation. Denoting the permutation matrix of π by P, define the graph D' with adjacency matrix $A_{D'} = P^{-1}A_D$. Then D' is loop-full, thus there exists $M' \in \mathrm{M}[D', q]$ with determinant $\mathrm{sign}(\pi)$. Finally, the matrix $M := PM'$ belongs to $\mathrm{M}[D, q]$ and has determinant 1. □

Recall that the term rank of a matrix is the maximum number of non-zero entries which are not in the same row or column. By the max-flow min-cut theorem, this is equal to the number of lines (rows and columns) necessary to cover all non-zero entries of the matrix. The term rank of the adjacency matrix of a graph is equal to the maximum number of pairwise independent arcs, where $uv, u'v'$ are independent if and only if $u \neq u'$ and $v \neq v'$; it is denoted as $\alpha_1(D)$ in [5].

Corollary 3.3 (Edmonds's theorem [22])**.** *The maximum possible rank of a real matrix with interaction graph D is equal to $\alpha_1(D)$. Moreover, the maximum is achieved by a matrix with entries in $\mathbb{Z}$.*

Corollary 3.4 ([5])**.** *The maximum possible rank of a network in $\mathrm{F}[D, q]$ is equal to $q^{\alpha_1(D)}$ for all $q \geq 3$. Moreover, the maximum is achieved by a linear function over $\mathbb{Z}_q$.*

3.2. Families of graphs with expansive networks over all alphabets

We exhibit two families of graphs which generalise the cycle, in the sense that the cycle belongs to either family and that every member of the family admits an expansive network over any alphabet (apart from one exception).

The first family is that of cycles with loops. Say $D = (V = [\![n]\!], E)$ is a **cycle with loops** if there exists $S \subseteq [\![n]\!]$ such that $E = \{(i, i + 1 \bmod n) : 0 \leq i < n\} \cup \{(s, s) : s \in S\}$. Say a cycle with loops is proper if $S \neq V$.

We shall repeatedly use the following facts, whose proofs are obvious and hence omitted. Firstly, the following are equivalent:

1. The XOR network on D is bijective.
2. The adjacency matrix A_D is nonsingular over GF(2).
3. D has an odd number of cycle decompositions.

Secondly, if D has a unique cycle decomposition, then the adjacency matrix A_D has determinant one over all rings $\mathbb{Z}_q$.

Proposition 3.5. *If D is a cycle with loops, then D admits an expansive linear network for any $q \geq 2$, unless D is an improper cycle with loops and $q = 2$.*

Proof. We recall that a linear network $f(x) = xM$ is expansive if for all $u \in [\![n]\!]$, the matrix M and the matrix

$$N_u^{(0)} = \left(\begin{array}{c|c|c|c} I_u & M_u & \dots & M_u^{n-1} \end{array} \right)$$

are nonsingular. If D is a proper cycle with loops, then let $M = A_D$. Since D has a unique cycle decomposition, A_D is nonsigular. Also, up to a permutation of columns, $N_u^{(0)}$ is upper triangular with all ones on the diagonal, hence its determinant is equal to one and $N_u^{(0)}$ is nonsingular.

If D is an improper cycle with loops, we see that it has exactly two cycle decompositions. As such, the XOR network is not bijective and D does not admit an expansive linear network for $q = 2$. For $q = 3$, let $a \in \mathbb{Z}_q \setminus \{0, 1\}$ be invertible, $b = 1 - a$ if n is odd and $b = a + 1$ if n is even, and

$$M = \begin{pmatrix} b & a & 0 & \cdots & 0 \\ 0 & 1 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 & 1 \\ 1 & 0 & \cdots & 0 & 1 \end{pmatrix},$$

then $\det(M) = 1$. Once again, $N_u^{(0)}$ is upper triangular, and $\det(N_u^{(0)})$ is a power of a, which shows that $N_u^{(0)}$ is nonsingular. □

The second family is that of cycles of cycles. Say D is a **cycle of cycles** if either it is a cycle or it is a union of $k \geq 2$ disjoint cycles $C_1, \dots, C_k$, linked as follows: for each cycle C_i there are two vertices u_i, v_i (which may be equal) such that $u_i v_{i+1} \in E$ for all $1 \leq i \leq k$ (computed cyclically). Say a cycle of cycles is proper if there exists i such that $u_i v_i \notin E$.

Proposition 3.6. *If D is a cycle of cycles, then D admits a linear expansive network for all $q \geq 2$ unless D is an improper cycle of cycles and $q = 2$.*

Proof. Let D be a proper cycle of cycles. Firstly, we verify that D has a unique cycle decomposition. This is true when D is a cycle. Otherwise, let i such that $u_i v_i \notin E$, then the successor w_i of u_i belongs to only one cycle, namely C_i. Once C_i is removed, it is then clear that v_{i+1} only belongs to one cycle, namely C_{i+1}, and so on. Thus, the XOR network on D is bijective. Conversely, if D is an improper cycle of cycles, then it has exactly two cycle decompositions, and hence the XOR network is not bijective. For $q \geq 3$, there always exists a linear bijective network by Theorem 3.2.

Let f be a linear bijective network on D. Suppose, for the sake of contradiction, that f is not expansive. Let x and v such that for all $t \geq 0$, $f_v^t(x) = 0$. We

consider two cases. Firstly, suppose that for all $1 \leq i \leq k$, there exists $t_i \geq 0$ such that $f_{u_i}^{t_i}(x) \neq 0$. Let v be any vertex, say it belongs to C_i; denote the vertices of C_i as $u_i, u_i + 1, \ldots u_i + l_i - 1$ and in particular $v = u_i + b$. We then have

$$f_{u_i+a}^{t_i+a}(x) \neq 0$$

for all $0 \leq a \leq l_i - 1$ and in particular $f_v^{t_i+b}(x) \neq 0$, which is the desired contradiction.

Secondly, suppose that there exists $1 \leq j \leq k$ such that $f_{u_j}^t(x) = 0$ for all $t \geq 0$. Then for all $t \geq l_j$, $f_{C_j}^t(x) = 0$. (Justify.) For any $t \geq l_j$, we have

$$0 = f_{v_j}^{t+1}(x) = f_{u_{j-1}}^t(x),$$

thus by a similar reasoning, $f_{C_{j-1}}^t(x) = 0$ for all $t \geq l_j + l_{j-1}$. By obvious induction, we obtain that $f^n(x) = 0$, which contradicts the fact that f is bijective. □

3.3. Characterization of graphs admitting expansive networks for some alphabet

We now characterize the graphs D which admit an expansive network over some alphabet. We can actually be more precise, and consider variations of our main definition without affecting the characterization. A network f is said to be **weakly expansive** if for all $x \neq y$ and all v, there exists $t \geq 0$ such that $f_v^t(x) \neq f_v^t(y)$. Note that a weakly expansive f does not have to be bijective. Recall that a network f is quasi-expansive (Definition 2.4) if for all $x \neq y$ and all v, there exists $t \geq 0$ such that $f_{N_{\text{in}}(v)}^t(x) \neq f_{N_{\text{in}}(v)}^t(y)$. It is not difficult to see that these definitions are not equivalent. However, the interaction graphs they characterize are the same as shown in the following theorem.

Theorem 3.7. *The following are equivalent for a graph D on $n \geq 2$ vertices.*

1. *D is strongly connected and coverable.*
2. *D admits an expansive network over some q.*
3. *D admits a quasi-expansive network over some q.*
4. *D admits a weakly expansive network over some q.*
5. *D admits a linear expansive network over any large enough finite field.*

Clearly, an expansive network is quasi-expansive and weakly expansive. Therefore this theorem follows from the next three results.

Lemma 3.8. *If D admits a quasi-expansive network, then D is strongly connected and coverable (or D has a single node).*

Proof. Let $f \in \mathrm{F}[D, q]$ for some $q \geq 2$. If D is not strongly connected, then let u and v such that there is no path from u to v in D. There is no path from u to $N_{\text{in}}(v)$ either. Then it is clear that for any $t \geq 0$, f_W^t does not depend on

x_u, where $W = N_{\text{in}}(v)$. In particular, if $x, y \in [\![q]\!]^n$ only differ in position u, we have $f_W^t(x) = f_W^t(y)$ for all $t \geq 0$. Therefore, f cannot be quasi-expansive.

Suppose D is not coverable, then by [14, Proposition 3.11.6] there exists $S \subseteq V$ such that $|N_{\text{out}}(S)| < |S|$. Choose any vertex $v \notin N_{\text{out}}(S)$ (v may be in S or not). By the pigeonhole principle there must exist two distinct configurations $x, y \in [\![q]\!]^n$ such that x and y differ only on S and $f(x)_{N_{\text{out}}(S)} = f(y)_{N_{\text{out}}(S)}$. But it also holds that $f(x)_i = f(y)_i$ for any $i \notin N_{\text{out}}(S)$ because $x_{N_{\text{in}}(i)} = y_{N_{\text{in}}(i)}$ since $N_{\text{in}}(i) \cap S = \emptyset$. We deduce that $f^t(x) = f^t(y)$ for all $t \geq 1$ and $x_{N_{\text{in}}(v)} = y_{N_{\text{in}}(v)}$ which proves that f is not quasi-expansive. □

Lemma 3.9. *If D admits a weakly expansive network, then D is strongly connected and coverable (or $D = K_1$).*

Proof. The proof is similar to that of Lemma 3.8. Again, it is clear that D must be strongly connected. If D is not coverable, then let $S \subseteq V$ such that $|N_{\text{out}}(S)| < |S|$. If $S = V$, then some vertex has no outgoing edge so the graph is not strongly connected. If $S \neq V$, then there exist distinct configurations x, y such that $x_S \neq y_S$ and $x_{V \setminus S} = y_{V \setminus S}$ and $f(x) = f(y)$. Thus, for any $v \notin S$ and any $t \geq 0$, $f_v^t(x) = f_v^t(y)$. □

We have no constructive method to produce an expansive network on a given strongly connected and coverable digraph. The next theorem shows their existence by a counting argument based on the Schwartz-Zippel Lemma. The hard part of the proof is to establish that some determinants are non-zero using the structure of the considered digraphs.

Theorem 3.10. *Any strongly connected and coverable graph D on n vertices admits an expansive linear network over* $\mathrm{GF}(q)$ *for any prime power $q \geq \frac{1}{2}(n^3 + n^2 + 4)$.*

Proof. We recall that by Lemma 2.2 a linear function $f(x) = xM$ is expansive if and only if for all $u \in [n]$, the matrix $N := N_u^{(1)} = \left(\begin{array}{c|c|c|c} M_u & M_u^2 & \dots & M_u^n \end{array} \right)$ is nonsingular. Our proof is nonconstructive: we shall see the nonzero coefficients of the matrix M as variables, then the determinant of N is a polynomial of these variables; if the field is large enough, then we can always evaluate that polynomial to something other than zero, provided it is not the null polynomial.

Let $\bar{C}_1, \dots, \bar{C}_s$ be a decomposition of the vertex set of D into cycles. We let $X(e) = \bar{\alpha}_k$ if e is one of the arcs in $\bar{C}_k$; otherwise, we give a different variable $X(e) = \bar{\beta}_e$ for any other arc e (and in particular for the chords of the cycles $\bar{C}_1, \dots, \bar{C}_s$). For any walk $W = e_1, \dots, e_L$ on D, we denote the monomial $X(W) = X(e_1)X(e_2)\cdots X(e_L)$. (The sum and the product of variables commute.)

We fix a vertex u, say it belongs to $\bar{C}_\sigma$. Let T be a spanning "tree of cycles" rooted at $\bar{C}_\sigma$. More precisely, T is a spanning subgraph of D which contains all the cycles $\bar{C}_1, \dots, \bar{C}_s$ and for any $k \neq \sigma$, there is exactly one arc leaving $\bar{C}_k$. (Such a tree of cycles can be easily constructed by contracting every cycle to a vertex and then building a spanning in-tree rooted at the vertex corresponding

to $\bar{C}_\sigma$.) It will be convenient to re-order the cycles according to the topological order in T. We then have $C_1 = \bar{C}_\sigma, C_2, \ldots, C_s$. We similarly re-define the variables: α_k is the variable for all the arcs in C_k ($1 \leq k \leq s$), while β_k is the variable corresponding to the arc leaving C_k in T ($2 \leq k \leq s$).

Recall that the determinant $\det(N_u^{(1)})$ is a sum over all permutations of products of terms. The main point of the proof is to show that $\det(N_u^{(1)})$ is not the null polynomial by exhibiting a monomial Y that appears only in the product corresponding to a particular permutation, hence no cancellation can occur in the sum over permutation defining $\det(N_u^{(1)})$ and Y indeed appears in $\det(N_u^{(1)})$. This monomial is obtained from canonical paths of particular lengths in the structure of tree of cycles above: they each consist in making a number of turns around some cycle and then taking the shortest path to u. Their precise description follows.

For $1 \leq k \leq s$, let L_k be the length of C_k and $\Lambda_k := L_1 + \cdots + L_{k-1}$ ($\Lambda_1 = 0$). We also denote the shortest path from C_k to u in T as W_k and we denote its length as λ_k and its monomial as $X_k = X(W_k)$; for $k = 1$, W_1 is the empty path thus $\lambda_1 = 0$ and $X_1 = 1$. It is easily seen that $\Lambda_k \geq \lambda_k$ for all k. We remark that for any distinct $v, v' \in C_k$, $d_T(v,u) \not\equiv d_T(v',u) \mod L_k$, where d_T denotes the distance in T. We can then denote the vertices of C_k according to their distance to u as follows: let the vertices in C_k be v_k^j for $j = 1, \ldots, L_k$, where $d_T(v_k^j, u) \equiv \Lambda_k + j \mod L_k$. From this definition we have $\Lambda_k + j \geq d_T(v_k^j, u)$ because $0 \leq d_T(v_k^j, u) - \lambda_k < L_k$ and $\Lambda_k + j - \lambda_k \geq 0$ and $\Lambda_k + j - \lambda_k \equiv d_T(v_k^j, u) - \lambda_k \mod L_k$.

For any row (vertex) v and column (time) t, we have $N(v,t) = \sum_W X(W)$, where the sum is taken over all walks from v to u of length t. Let us consider $v = v_k^j$ and $t = \Lambda_k + j$. There is a canonical walk from v to u of time t: going round the cycle C_k as many times as possible and then take the shortest path from C_k to u, which yields the term $\alpha_k^{t-\lambda_k} X_k$. All the other walks either remain in T, but if so do not use α_k as many times, or leave T.

This yields: $N(v_k^j, \Lambda_k + j) = \alpha_k^{\Lambda_k + j - \lambda_k} X_k + \Gamma + \Delta$, where all the terms in Γ contain a variable outside of those of T, and the degree of α_k in Δ is at most $\Lambda_k + j - 1$. Therefore, the product

$$\prod_{\substack{1 \leq k \leq s \\ 1 \leq j \leq L_k}} N(v_k^j, \Lambda_k + j)$$

contains the monomial $Y := \prod_{k=1}^s \alpha_k^{d_k} X_k^{L_k}$, where $d_k := L_k \left(\frac{1}{2}(L_k + 1) + \Lambda_k - \lambda_k \right)$.

The term Y contributes to the determinant of N, for the permutation ρ of $[n]$, defined as $\rho(v_k^j) = \Lambda_k + j$. We now prove that Y does not appear in any other product of entries that contribute to the determinant of N. More precisely, we prove by induction on k from s down to 1 that if any permutation π of $[n]$ produces for every k a term only involving variables from T where α_k has degree d_k, then $\pi(v) = \rho(v)$ for all $v \in C_k$.

Let us prove the case $k = s$. Let $\pi(C_s) = \{t_1, \ldots, t_{L_s}\}$ with $t_1 < \cdots < t_{L_s}$. Clearly, we only need to consider walks in T. According to the topological

order of cycles in T, there is no path from C_i to C_j if $i < j$. In particular, the rows of N corresponding to a vertex outside of C_s does not contain α_s. Thus, the degree of α_s is at most $(t_1 - \lambda_s) + \cdots + (t_{L_s} - \lambda_s)$. We then have $t_1 + \cdots + t_{L_s} - L_s\lambda_s \geq d_s = L_s\left(\frac{1}{2}(L_s+1) + \Lambda_s\right) - L_s\lambda_s$, which implies $t_j = \Lambda_s + j$ for $j = 1, \ldots, L_s$. Moreover, the degree of α_s in $N(v_s^i, \Lambda_s + j)$ is equal to $\Lambda_s + j - \lambda_s$ if and only if $i = j$. This implies that $\pi(v_s^j) = \Lambda_s + j$ for all j. The inductive step is similar and hence omitted.

We have thus shown that $\det(N_u^{(1)})$ is a nonzero polynomial in the variables $\{X(e) : e \in E\}$. Its degree is clearly $d := n(n+1)/2$. By the Schwartz-Zippel Lemma [23, Theorem 7.1.4], there are at most $d(q-1)^{|E|-1}$ choices for the values of $X(e)$ for which $\det(N_u^{(1)}) = 0$. Thus, there are at most $nd(q-1)^{|E|-1}$ choices for the values of $X(e)$ for which $\det(N_u^{(1)}) = 0$ for some $u \in [n]$. Since $q - 1 > nd$, we have $(q-1)^{|E|} > nd(q-1)^{|E|-1}$, and hence there exists a choice of values for all the variables $X(e)$ such that $\det(N_u^{(1)}) \neq 0$ for all u. □

We highlight two consequences of our result. Firstly, we comment on the alphabets for which a strongly connected and coverable D admits a linear expansive network. The **cartesian product** of two networks $f \in \mathrm{F}(n, q)$ and $g \in \mathrm{F}(n, r)$ is defined as follows. We view $[\![qr]\!] \cong [\![q]\!] \times [\![r]\!] = \{(a^1, a^2) : a^1 \in [\![q]\!], a^2 \in [\![r]\!]\}$, then $f \times g = h \in \mathrm{F}(n, qr)$ with $h(x^1, x^2) = (f(x^1), g(x^2))$. Many properties are preserved by cartesian products: if f and g are expansive, then so is $f \times g$; if f and g are linear, then so is $f \times g$; if f and g have interaction graph D, then so does $f \times g$. In particular, if D admits a linear expansive network over alphabets of size q and r, then it admits a linear expansive network over an alphabet of size qr.

Corollary 3.11. *For any strongly connected and coverable D, the set of alphabet sizes q for which there exists a linear expansive network in $\mathrm{F}[D, q]$ has positive density.*

Proof. Denote the prime numbers as $p_1 < p_2 < \ldots$. Say p_j is the largest prime no greater than $q := \frac{1}{2}(n^3 + n^2 + 4)$, then let $d_i = \lceil \log_{p_i} q \rceil$ for all $i \leq j$. Then D admits an expansive network on any multiple of $Q := \prod_{i=1}^{j} p_i^{d_i}$. □

We actually conjecture that for any strongly connected and coverable D, there exists q such that D admits an expansive network over all alphabets of size greater than q.

A corollary of Theorem 3.10 is that choosing a linear network at random will almost surely yield an expansive network when q is large enough. Even more strikingly, we can define the following strategy to construct entire families of expansive networks. For a given n and prime power q, the Random-Linear-Strategy first chooses a random matrix $M \in \mathrm{GF}(q)^{n \times n}$ whose entries are all nonzero. Then for a given graph D on $[n]$, the strategy yields the linear network $f_{M,D}(x) = x(M \odot A_D)$ and $\odot$ denotes the Hadamard product of matrices. The following corollary shows that the probability to get an expansive network for all strongly connected and coverable graphs goes to 1 as the alphabet size goes to infinity.

Corollary 3.12. *The Random-Linear-Strategy produces from a single random matrix M an expansive network $f_{M,D}$ for all strongly connected and coverable graph D on n vertices with probability at least $1 - \Delta/(q-1)$, where $\Delta = 2^{n^2-1}n^2(n+1)$.*

Proof. Let $\alpha = \{\alpha_{ij} : i, j \in [\![n]\!]\}$ be an outcome of the Random-Linear-Strategy, where α_{ij} is a nonzero element of GF(q) for all q. For any strongly connected and coverable graph D on n vertices, there are at most $n \cdot n(n+1)/2 \cdot (q-1)^{n^2-1}$ choices for α which do not yield an expansive network on D. Since there are at most 2^{n^2} choices for D, there are at most $\Delta(q-1)^{n^2-1}$ choices of α which do not produce an expansive network for all D. Thus, the probability of success is at least $1 - \Delta(q-1)^{n^2-1}/(q-1)^{n^2}$. □

4. Alphabet size and nonexistence of expansive networks

We only consider strongly connected and coverable graphs from now on. For any graph D, we denote the set of expansive (abelian expansive, respectively) networks in $\mathrm{F}[D, q]$ as $E[D, q]$ ($EA[D, q]$, respectively). Our nonexistence results are based on the following family of graphs. Consider for any $n \geq 2$ the graph $G_n = (V_n = \{0, 1, \ldots, n\}, E_n)$ where $E_n = \{(0, i), (i, 0), (i, i) : 0 \leq i \leq n\}$.

Any network with a small enough alphabet and with interaction graph G_n must have symmetries in its local functions f_i for $i \neq 0$ (counting argument). The following theorem uses this idea to show that expansivity is impossible with small alphabets on graphs G_n.

Theorem 4.1. *For all q, there exists n_0 (triply exponential in q) such that, for all $n \geq n_0$, $E[G_n, q] = \emptyset$.*

Proof. We first show that any $f \in \mathrm{F}[G_n, q]$ has a lot of initial configurations reaching cycles of constant size in constant time (*i.e.* independent of n). To make a precise statement, denote for any $\phi \in [\![q]\!]^{[\![q]\!]^2}$ the set of automata in f whose local update map is ϕ: $V_\phi = \{i : 0 < i \leq n \text{ and } \forall x, f_i(x) = \phi(x_i, x_0)\}$. Choose any ϕ, any $V \subseteq V_\phi$ and define the configuration $c_{\phi,V} \in [\![q]\!]^{[n]}$ by:

$$c_{\phi,V}(j) = \begin{cases} 0 & \text{if } j \notin V \\ 1 & \text{else.} \end{cases}$$

We claim that the orbit under f of any such $c_{\phi,V}$ has length at most $p = q^{q^{q^2}+2}$. Indeed, by induction on t, it holds that $f^t(c_{\phi,V})_i = f^t(c_{\phi,V})_j$ if $\{i, j\} \subseteq V_{\phi'}$ for $\phi' \neq \phi$, or $\{i, j\} \subseteq V$, or $\{i, j\} \subseteq V_\phi \setminus V$ (it is true at $t = 0$ and preserved because two automata $\{i, j\} \subseteq V_{\phi'}$ apply the same update map ϕ'). It follows that there are at most $q^{q^{q^2}+2}$ different configurations in the orbit of $c_{\phi,V}$, which proves the claim.

Now fix q, let $p = q^{q^{q^2}+2}$ and $l > \lceil \log_2(q^{2p}) \rceil$ and choose $n \geq lq^{q^2}$. By choice of n there must be $\phi \in [\![q]\!]^{[\![q]\!]^2}$ such that $|V_\phi| \geq l$. Thus, there are 2^l choices of

$V \subseteq V_\phi$ yielding 2^l distinct configurations of the form $c_{\phi,V}$. For any configuration c, define $\rho(c) := \rho_0^{(2p)}(c)$ the trace of length $2p$ at node 0. By choice of l there must be $V, V' \subseteq V_\phi$ with $V \neq V'$ such that $\rho(c_{\phi,V}) = \rho(c_{\phi,V'})$ (because ρ can take only q^{2p} different values). Note that using the notation from section 5, we thus have two distinct configurations $x = c_{\phi,V}$ and $y = c_{\phi,V'}$ such that $\tau_0(x, y) \geq l_x + l_y$, which contradicts the fact that $\tau_v(x, y) < l_x + l_y$, as shown in the proof of Theorem 5.4. □

We now prove that the bound on the smallest n such that there exists G on n vertices with no expansive networks over $[\![q]\!]$ can be significantly lowered if we only consider linear networks. We give a proof that actually holds for abelian networks with a quasi-polynomial bound.

Theorem 4.2. *For any $q \geq 2$ and any $n > q^{2\log(q)}$ it holds $EA[G_n, q] = \emptyset$.*

Proof. Let N_q denote the maximum number of endomorphisms of an abelian group of order q. By the decomposition theorem of Abelian groups into products of cyclic groups, one sees that an endomorphism is determined by its value on at most $\log(q)$ elements (elements equal to the generator on one component of the product and 0 on the others), thus $N_q \leq q^{\log(q)}$. Let $n > q^{2\log(q)} \geq N_q^2$. Let A be an abelian group of order q and $f \in \mathrm{F}[G_n, q]$ be an endomorphism of A^{n+1}. Then there exist i and j such that $f_i(x) = g(x_i) + h(x_0)$, $f_j(x) = g(x_j) + h'(x_0)$ and $f_0(x) = e(x_i) + e(x_j) + h''(x_{\{0,\dots,n\}\setminus\{i,j\}})$ for some endomorphisms g, e, h, h' and h''. Consider a nonzero configuration x such that $x_i + x_j = 0$ and $x_u = 0$ for any other vertex u, we then have

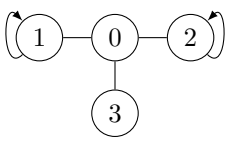
$$f_i(x) + f_j(x) = g(x_i + x_j) + h(x_0) + h'(x_0) = 0,$$
$$f_0(x) = e(x_i + x_j) + h''(x_{\{0,\dots,n\}\setminus\{i,j\}}) = 0.$$

By induction, we have $f_0^t(x) = 0$, thus f is not expansive. □

The proof can be easily adapted for linear networks, thus yielding a polynomial bound on the smallest n for which G_n admits no linear network over an alphabet of size q.

Corollary 4.3. *The graph G_n admits no linear expansive network for q whenever $n > (q-1)^2$.*

We conjecture that in fact, there is a sharp distinction between admitting an expansive network and admitting an abelian expansive network: for all q, there exists D such that $E[D, q] \neq \emptyset$ but $EA[D, q] = \emptyset$. We make some progress towards this conjecture by showing that it holds for all $q \equiv 2 \mod 4$. Let G be the graph on four vertices displayed below:



Proposition 4.4. *We have $E[G,q] \neq \emptyset$ for all $q \geq 2$. However, $EA[G,q] \neq \emptyset$ if and only if $q \not\equiv 2 \mod 4$.*

Proof. Firstly, we verify that G admits no abelian expansive network for $q = 2$. For $q = 2$, the only abelian network is the XOR network $f(x) = xA_G$. The configuration $x = (0, 1, 1, 0)$ is a fixed point of the XOR network, thus the latter is not expansive. More generally, for any $q = 2k$ for k odd, any abelian network $h \in \mathrm{F}(n, 2k)$ decomposes as $h = f \times g$, where $f \in \mathrm{F}(n, 2)$ and $g \in \mathrm{F}(n, k)$ are both abelian. We thus obtain that G admits no abelian expansive network for any $q \equiv 2 \mod 4$.

Secondly, we show that there exists an abelian expansive over G for all $q \not\equiv 2 \mod 4$. We only need to prove the case for non-binary finite fields, the general case following by cartesian product. Let $q \neq 2$ be a prime power and let $\alpha \neq \{0, 1\}$ be an element of $\mathrm{GF}(q)$. Let $f(x) = xM$, where

$$M = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & \alpha & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}.$$

Clearly, $\det(M) = -\alpha$ and hence f is bijective. After some straightforward calculations, we obtain

$$N_0 = \begin{pmatrix} 1 & 0 & 3 & \alpha+1 \\ 0 & 1 & 1 & 4 \\ 0 & 1 & \alpha & \alpha^2+3 \\ 0 & 1 & 0 & 3 \end{pmatrix}, \qquad \det(N_0) = \alpha^2 - \alpha;$$

$$N_1 = \begin{pmatrix} 0 & 1 & 1 & 4 \\ 1 & 1 & 2 & 3 \\ 0 & 0 & 1 & \alpha+1 \\ 0 & 0 & 1 & 1 \end{pmatrix}, \qquad \det(N_1) = \alpha;$$

$$N_2 = \begin{pmatrix} 0 & 1 & \alpha & \alpha^2+3 \\ 0 & 0 & 1 & \alpha+1 \\ 1 & \alpha & \alpha^2+1 & \alpha^3+2\alpha \\ 0 & 0 & 1 & \alpha \end{pmatrix}, \qquad \det(N_2) = -1;$$

$$N_3 = \begin{pmatrix} 0 & 1 & 0 & 3 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & \alpha \\ 1 & 0 & 1 & 0 \end{pmatrix}, \qquad \det(N_3) = 1 - \alpha.$$

All determinants are nonzero, thus f is expansive.

Thirdly, for $q = 2$, it is straightforward to check that the following network

is indeed expansive.

$$\begin{aligned} f_0(x) &= x_1x_2 + x_3 + 1 \\ f_1(x) &= x_0 + x_1 \\ f_2(x) &= x_0 + x_2 + 1 \\ f_3(x) &= x_0. \end{aligned}$$

Again, combining our previous results and using the cartesian product, we conclude that G admits an expansive network for all $q \geq 2$. □

5. Expansion time

Consider some expansive network f. For any node v and any configuration x, it is clear that the trace $\rho_v(x)$ is periodic. In particular, let $O_x = \{f^t(x) : t \geq 1\}$ be the orbit of x, then the period of the trace of x is equal to the size $l_x = |O_x|$ of its orbit (if it were shorter of length l, then x and $f^l(x)$ would be two distinct configurations of same trace).

For any expansive network $f \in \mathrm{F}(n, q)$, any different $x, y \in [\![q]\!]^n$ and any $v \in [n]$, let

$$\tau_v(x, y) = \min \left\{ t \geq 1 : f_v^t(x) \neq f_v^t(y) \right\}.$$

The **expansion time** of f is then $T(f) := \max_{x \neq y \in [\![q]\!]^n, v \in [n]} \tau_v(x, y)$. This is the shortest time for which the temporal evolution of x_v determines x completely, for any x and any v. For any v, it is clear that if the function $\rho_v^{(T)}$ is injective, then $T \geq n$, thus $T(f) \geq n$. Say f is **strongly expansive** if it is expansive and $T(f) = n$. Lemma 2.2 then shows that any expansive field linear network is strongly expansive. Strongly expansive networks can be viewed as follows. For any $x \in [\![q]\!]^n$, consider the matrix

$$M_x = \begin{pmatrix} f_1(x) & f_2(x) & \dots & f_n(x) \\ f_1^2(x) & f_2^2(x) & \dots & f_n^2(x) \\ \vdots & \vdots & \dots & \vdots \\ f_1^n(x) & f_2^n(x) & \dots & f_n^n(x) \end{pmatrix}.$$

Then f is bijective if and only if we can recover x from any *row* of M_x, while f is strongly expansive if and only if we can recover x from any *column* of M_x.

The expansion time is the minimum value of T such that one can recover any x from the first T time steps of its trace at v. For a given x and a given v, that particular time may be smaller than n. as shown in the following example.

Example 5.1. *Let $f \in \mathrm{F}(3, 2)$ be as follows*

x	$f(x)$
000	*001*
001	*110*
010	*101*
011	*111*
100	*011*
101	*010*
110	*000*
111	*100*

x	$(f_1(x), f_1^2(x), f_1^3(x), f_1^4(x))$
000	***0100***
001	***100****1*
010	***1010***
011	***11****01*
100	***011****0*
101	***0101***
110	***00****10*
111	***1011***

It can be checked that f is indeed expansive, with expansion time $T(f) = 4$ (and hence f is not strongly expansive). In the traces at vertex $v = 1$ shown above (the part of the trace that allows to recover the initial state is highlighted), it appears that the states 011 *and* 110 *could be recovered after only two time steps.*

However, the expansion time is "universal" for strongly expansive networks: for any v and any x, one must wait n time steps before being able to recover x.

Proposition 5.2. *If f is strongly expansive, then for any $v \in [n]$ and $x \in [\![q]\!]^n$, there exists $y \neq x$ such that $\tau_v(x, y) = n$.*

Proof. If f is strongly expansive, then for any v, the function $\rho_v^{(n)}$ is surjective. Suppose, for the sake of contradiction, that there exists x such that for any $y \neq x$, $\rho_v^{(n-1)}(x) \neq \rho_v^{(n-1)}(y)$. Let $a \neq f_v^n(x)$, then there is no y such that $\rho_v^{(n)}(y) = (\rho_v^{(n-1)}(x), a)$, thus contradicting surjectivity. □

In order to highlight the specificity of strongly expansive networks, we now show that the maximum possible expansion time for expansive network is almost q^n.

Example 5.3 (Expansive counter)**.** *We construct an expansive network f in* $\mathrm{F}(n, q)$ *with expansion time $T(f) \geq q^n - q - 1$. Intuitively, this network is the successor function of a particular enumeration of $[\![q]\!]^n$, which can be viewed as a "twisted lexicographic order." More formally, for any integer $0 \leq a \leq q^n - 1$, say $a = a_1 + a_2 q + \cdots + a_n q^{n-1}$, let $x^a = (x_1^a, \ldots, x_n^a) \in [\![q]\!]^n$ be defined as $x_n^a = a_n$ and for $1 \leq i \leq n - 1$,*

$$x_i^a = \begin{cases} q-2 & \text{if } a_{i+1} = \cdots = a_n = q-1 \text{ and } a_i = q-1 \\ q-1 & \text{if } a_{i+1} = \cdots = a_n = q-1 \text{ and } a_i = q-2 \\ a_i & \text{otherwise.} \end{cases}$$

Then let $f(x^a) = x^{a+1 \bmod q^n}$. Since the maps $a \mapsto a + 1 \bmod q^n$ and $a \mapsto x^a$ are bijective, f is well-defined by the previous formula and also bijective.

The next theorem establishes precise bounds on the maximum possible expansion time. The upper bound uses arguments similar to the theorem of Fine and Wilf on words.

Theorem 5.4. *For all n and q, the maximum $T(f)$ over all expansive $f \in \mathrm{F}(n,q)$ is between $q^n - q - 1$ and $q^n - 1$. The lower-bound is granted by Example 5.3 which verifies $T(f) \geq q^n - q - 1$.*

Proof. Upper bound. Let $x \neq y$ with $l_x \leq l_y$; denote $\tau = \tau_v(x,y)$.

Case 1: $l_x \mid l_y$. We first prove that $\tau \leq l_y$. Suppose that this is not the case, i.e. $f_v^t(x) = f_v^t(y)$ for all $1 \leq t \leq l_y$. Then $\rho_v(x) = \rho_v(y)$, which contradicts the expansivity of f. Thus, $\tau \leq l_y \leq q^n$. Suppose that $\tau = l_y = q^n$, then f is a cyclic permutation of $[\![q]\!]^n$ and the trace $\rho_v(x)$ is a cyclic shift of $\rho_v(y)$, and their only difference is in position q^n, i.e $x_v = a \neq y_v = b$. Let $N = |\{t : 1 \leq t \leq q^n - 1, f_v^t(x) = a\}|$ denote the number of times the trace of x is equal to a until time $q^n - 1$. We then have $N = q^{n-1} - 1$. However, N also counts the number of times the trace of y is equal to a until time $q^n - 1$; we obtain $N = q^{n-1}$, which is the desired contradiction.

Case 2: $l_x \not| l_y$. We prove that $\tau \leq l_x + l_y - \gcd(l_x, l_y) - 1$ which is sufficient to get the upper bound of the theorem since in this case x and y have disjoint orbits and therefore $l_x + l_y \leq q^n$. Suppose, for the sake of contradiction, that $\tau \geq l_x + l_y - \gcd(l_x, l_y)$. We shall reason in terms of blocks of length $\gcd(l_x, l_y)$. Say the first period of the trace of x is $X = u_1, \ldots, u_{|X|}$ and that of y is $Y = u_1, \ldots, u_{|Y|}$ (this is coherent since X is a prefix of Y). We then have $|X| = l_x / \gcd(l_x, l_y)$ and $|Y| = l_y / \gcd(l_x, l_y)$; these two are coprime. Let $|Y| = \alpha|X| + a$ for $0 \leq a < |X|$ and $|X| = \beta a + b$ for $0 \leq b < a$, then a and b are coprime.

Claim 5.5. *Let $u := u_1, \ldots, u_a$ and $u' := u_1, \ldots, u_b$. Then $X = u^\beta, u'$ and $Y = X^\alpha, u$.*

Proof. Clearly, we have $Y = X^\alpha, v$ for $v = u_{\alpha|X|+1}, \ldots, u_Y$. At times $\alpha|X| + 1$ to $\alpha|X| + a$, the trace of x describes u, thus $v = u$. This proves the second claim. Similarly, at times $|Y| + 1 = \alpha|X| + a + 1$ to $|Y| + a = \alpha|X| + 2a$, the trace of y describes u, thus X begins with u, u. By easy induction, we prove that u is repeated throughout X and we obtain $X = u^\beta, u'$. □

We now focus on times from $t := |X| + |Y| - a - b + 1$ to $t + a + b - 1 = |X| + |Y|$. The trace of x describes $u_1, \ldots, u_b, u_1, \ldots, u_{a-1}$, while the trace of y describes $u_1, \ldots, u_a, u_1, \ldots, u_{b-1}$. For the times from $t + b + 1$ to $t + a$, we obtain $u_i = u_{i+b}$ for all $1 \leq i \leq a - b$; for the times from $t + a + 1$ to $t + a + b - 1$, we obtain $u_j = u_{j-a+b}$ for all $a - b + 1 \leq j \leq a - 1$. Since b is coprime to a, it is easily checked that we obtain $u_1 = \cdots = u_a$. Thus, $X = u_1, \ldots, u_1$, which contradicts its period.

Lower bound. Let f be the network of Example 5.3. As already said, f is bijective. We now prove that f is expansive. We only need to show that for any $1 \leq e \leq \lfloor q^n/2 \rfloor$ and any $v \in [n]$, there exists $0 \leq t \leq q^n - 1$ such that $x_v^t \neq x_v^{e+t}$. Let k be the largest number such that q^k divides e. For $1 \leq v \leq k$, we have $x_v^{q^n - 1 - e} = q - 1$ and $x_v^{q^n - 1} = q - 2$, while for $k + 1 \leq v \leq n$, we have $x_v^{q^{v-1} - 1} = 0$ and $x_v^{q^{v-1} - 1 + e} \neq 0$. Finally, it is easily verified that $\tau_1(x^{q^n - 1}, x^{q-1}) = q^n - q - 1$. □

6. Expansion frequency

In the previous section, we have shown that we may have to wait until n time steps in order to differentiate a particular pair x, y of distinct states. However, that difference may occur frequently after its first occurrence. In this section, we are then interested at how often we see a difference between the orbits of x and y at some given node v.

For all distinct $x, y \in [\![q]\!]^n$ and all $v \in [n]$, let $\phi_v(x,y) := \frac{d_{\mathrm{H}}(\rho_v(x)^{(l_x l_y)}, \rho(y)^{(l_x l_y)})}{l_x l_y}$, where d_{H} denotes the Hamming distance. We then define the **expansion frequency** of f as

$$\Phi(f) = \min_{x \neq y \in [\![q]\!]^n, v \in [n]} \phi_v(x,y).$$

It is clear that $\frac{1}{T(f)} \leq \Phi(f) \leq 1$. However, $\Phi(f)$ itself can be as close to 1 as possible.

The upper bound in the following theorem is obtained through Berlekamp's generalisation of the Plotkin bound applied to the set of (long) traces at a given node seen as a code. Another link between variants of expansivity and codes is presented in section 8.

Theorem 6.1. *For any expansive network f, $\Phi(f) \leq \frac{q^n - q^{n-1}}{q^n - 1}$. Equality is achieved for all n and all prime powers q by some field linear network.*

Proof. Upper bound. Let N be the product of all the orbit lengths under f, and consider the code $C = \{\rho_v^{(N)}(x) : x \in [\![q]\!]^n\}$ of length N over $[\![q]\!]$. Since $T(f) \leq N$, all traces are distinct and hence $|C| = q^n$.

Claim 6.2. *The minimum distance of C is bounded by: $d_{\min}(C) \leq \delta := \frac{(q-1)Nq^{n-1}}{q^n - 1}$*

Proof. Berlekamp's generalisation of the Plotkin bound in [24] shows that for any code C of length N over $[\![q]\!]$ and minimum distance d, we have $|C| \leq \frac{dq}{dq - N(q-1)}$, provided the denominator is positive. Since $\delta q > N(q-1)$, we can use Berlekamp's generalisation of the Plotkin bound. In particular, if $d_{\min}(C) = d > \delta$, then $|C| \leq \frac{dq}{dq - N(q-1)} < \frac{\delta q}{\delta q - N(q-1)} = q^n$, which is a contradiction. Thus, $d \leq \delta$. □

By definition, there exists a pair $x, y \in [\![q]\!]^n$ such that $d_{\mathrm{H}}(\rho_v^{(N)}(x), \rho_v^{(N)}(y)) = d_{\min}(C)$. We obtain $\phi_v(x,y) \leq \frac{\delta}{N} = \frac{(q-1)q^{n-1}}{q^n - 1}$.

Achievability. Consider the q-ary image of the mapping $\xi \mapsto \alpha\xi$ in $\mathrm{GF}(q^n)$, where α is a primitive element of the field. This is a linear function in $\mathrm{F}(n,q)$, with 0 as its unique fixed point. For any nonzero $x \in \mathrm{GF}(q^n)$, the orbit of x contains all $q^n - 1$ nonzero elements of $\mathrm{GF}(q)^n$. Therefore, for any $x \neq 0$ and v, $\phi_v(x,0) = \frac{(q-1)q^{n-1}}{q^n - 1}$. □

On the other extreme, example 5.3 yields a network with expansion frequency of $2/q^n$.

7. PSPACE-completeness

In this section, we are interested in the problem of deciding whether a given network is expansive or not. Formally, we define the decision problem EXPAN as follows:

- **Input** : a triple (q, n, f) where $f : [\![q]\!]^n \to [\![q]\!]^n$ is given by circuits computing f_i for each i.
- **Question** : is f expansive?

The goal of this section is to prove that problem EXPAN is PSPACE-complete. Our proof proceeds by reduction from problem QBF (quantified Boolean formula) which is PSPACE-complete [25]. The simplest expansive network is the rotation map: $(q_1, \ldots, q_n) \mapsto (q_2, \ldots, q_n, q_1)$ (see section 3.2). The simplest non-expansive network is the identity map. The rough idea of our reduction is to construct an automata network with a special component of states (called *cycle configuration* below) and with the following behavior: repeatedly test by a brute force algorithm whether the QBF is true, and each time the test concludes 'true' do a rotation on the special component, otherwise let the special component unchanged. Thus, if the QBF is false, the constructed network is certainly not expansive (identity map on the special component). If, on the contrary, the QBF is true, then the network will repeatedly apply a rotation on the special component, ensuring that if two initial configurations differ on this component then their traces at any node will also differ. This is of course not enough to conclude: firstly, a pair of initial configurations might differ only outside the special component, and secondly the conclusion of the QBF test cannot be trusted if the algorithm was not initialized correctly. To ensure that the network is globally expansive in the case where the QBF is true, two additional properties will be granted:

1. the component of states used to perform the QBF test will itself be "expansive" (differences in the initial configurations in these components must be visible in the trace at any node) ;
2. the QBF test will self-detect bad initialization and, in this case, a rotation on the special component will be applied repeatedly.

The first key ingredient of our construction is the existence of expansive networks which implement counters (Lemma 7.1): using such expansive counters as a primitive everywhere will essentially ensure the first property above. The second key ingredient is the QBF test algorithm. It is a brute force algorithm with as many nested loops as variables in the QBF. At each level it counts how many valuation of a variable makes a subformula true to deduce truth at the upper level depending on the corresponding quantifier (we want two correct valuations for a $\forall$ quantifier and at least one for a $\exists$ quantifier). Each level is implemented using two variables: a loop counter acting like an instruction

counter, and a truth counter with is used to count the number of correct valuations. Loop counters have a completely rigid behavior independent of the QBF, they just indicate the progression of the test in the nested loops. Truth counters however depend on the QBF and their initialization is critical for the algorithm to give a correct answer. The self-detection for bad initialization will consist in double counting in each loop: increment the counter for each correct valuation, then use counter value to decide truth, then decrement the counter for each correct valuation, then test if counter value is zero (good initialization) or not and act correspondingly. To give a more concrete intuition before entering into the detailed construction, suppose the QBF is $\forall x_1, \exists x_2, \forall x_3, \phi(x_1, x_2, x_3)$ where ϕ is quantifier-free. Then the algorithm looks roughly like this[1]:

`algorithm:` do forever `level1()`

`level1()`: *(test truth of the whole QBF)*

1. if `level2`(0) then increment `TruthCounter1`
2. if `level2`(1) then increment `TruthCounter1`
3. if `TruthCounter1`= 2 then do rotation *(QBF considered true)*
4. if `level2`(0) then decrement `TruthCounter1`
5. if `level2`(1) then decrement `TruthCounter1`
6. if `TruthCounter1`$\neq$ 0 then do rotation *(bad initialization detected)*

`level2`(x_1): *(test truth of subformula $\exists x_2, \forall x_3, \phi(x_1, x_2, x_3)$)*

1. if `level3`(x_1, 0) then increment `TruthCounter2`
2. if `level3`(x_1, 1) then increment `TruthCounter2`
3. if `TruthCounter2`$\geq$ 1 then `test2`=true else `test2`=false
4. if `level3`(x_1, 0) then decrement `TruthCounter2`
5. if `level3`(x_1, 1) then decrement `TruthCounter2`
6. if `TruthCounter2`$\neq$ 0 then do rotation *(bad initialization detected)*
7. return `test2` *(truth of subformula)*

`level3`(x_1, x_2): *(test truth of subformula $\forall x_3, \phi(x_1, x_2, x_3)$)*

1. if $\phi(x_1, x_2, 0)$ is true then increment `TruthCounter3`
2. if $\phi(x_1, x_2, 1)$ is true then increment `TruthCounter3`
3. if `TruthCounter3`= 2 then `test3`=true else `test3`=false
4. if $\phi(x_1, x_2, 0)$ is true then decrement `TruthCounter3`

[1]To help readability we use pseudo-code with call/return of subroutines instead of loops with global variables. Not that local variables `test2` and `test3` are artifacts of the pseudo-code and are not present in the real construction.

5. if $\phi(x_1, x_2, 1)$ is true then decrement `TruthCounter3`
6. if `TruthCounter3`$\neq 0$ then do rotation *(bad initialization detected)*
7. return `test3`*(truth of subformula)*

We now proceed to the detailed description of our construction, starting from expansive counters.

Lemma 7.1 (Expansive counters)**.** *For any q and any n there exists $\chi_{q,n} : [\![q]\!]^n \to [\![q]\!]^n$ an expansive network for which all configurations belong to the same cyclcic orbit and with an ordering map $\nu_{q,n} : [\![q]\!]^n \to [\![q^n]\!]$ verifying $\forall x \in [\![q]\!]^n : \nu_{q,n}(\chi_{q,n}(x)) = \nu_{q,n}(x)+1 \bmod q^n$. $\chi_{q,n}$ has an expansion time of at most q^n. Moreover, for any fixed q, $\nu_{q,n}$ is computable by circuits of size polynomial in n, and there is an algorithm that given n compute in time polynomial in n the circuits representing $\chi_{q,n}$ and $\nu_{q,n}$.*

Proof. The lemma follows from Example 5.3 which is expansive as shown in Theorem 5.4. Let $\chi_{q,n}$ the network of the example and denote by ϕ the map $a \mapsto x^a$ used in its definition, and let ρ be the map $a \mapsto a + 1 \bmod q^n$ on $[\![q^n]\!]$. The orbits of ρ obviously consist in a single cycle. The example shows that $\chi_{q,n}$ is actually conjugated to ρ, meaning that $\phi^{-1} \circ \chi_{q,n} \circ \phi = \rho$. So the map $\nu_{q,n} = \phi^{-1}$ verifies the property stated in the lemma. It also follows that the orbits of $\chi_{q,n}$ consist in a single cycle. It is clear that ϕ and ϕ^{-1} and ρ have polynomial size circuits. Therefore it is also the case for $\chi_{q,n}$ which is a composition of these maps. Finally, one should be easily convinced that there is an algorithm that given n computes the circuits we are speaking about. □

Equipped with such expansive counters, we can now construct a network that implement the brute force algorithm to test a quantified Boolean formula. More precisely, given any quantified Boolean formula

$$\Psi = Q_0 x_0, Q_1 x_1, ..., Q_{n-1} x_{n-1} \phi(x_0, ..., x_{n-1})$$

(where each Q_i is either $\exists$ or $\forall$ and ϕ is quantifier-free) we build $f_\Psi : [\![q]\!]^n \to [\![q]\!]^n$ where $q = 2^{3n+1}$ as follows.

To simplify notations, we see any $x \in [\![q]\!]^n$ as a $n \times (3n + 1)$ array of elements of $[\![2]\!]$ and use the notation $x_{i,j}$ with $i \in [\![n]\!]$ and $j \in [\![3n + 1]\!]$ so that node i of the automata network in configuration x holds the vector of states $(x_{i,0}, \ldots, x_{i,3n}) \in [\![q]\!]$.

We want to interpret any configuration $x \in [\![q]\!]^n$ as $2n + 1$ configurations distributed over the network: n configurations of $[\![4]\!]^n$ called *loop counters*, n configurations of $[\![2]\!]^n$ called *truth counters* and a single configuration of $[\![2]\!]^n$ called the *cycle configuration*. Intuitively, to each variable of the formula Ψ is attached a loop counter and a truth counter, whose role is to implement the brute force algorithm sketched above. More precisely, for any $0 \leq k < n$ we define the following maps:

- the k^{th} loop counter map $L_k : [\![q]\!]^n \to [\![4]\!]^n$ verifying

$$L_k(x) = (2x_{0,3k} + x_{0,3k+1}, \ldots, 2x_{n-1,3k} + x_{n-1,3k+1}) \in [\![4]\!]^n,$$

- the k^{th} truth counter map $T_k : [\![q]\!]^n \to [\![2]\!]^n$ verifying

$$T_k(x) = (x_{0,3k+2}, \ldots, x_{n-1,3k+2}) \in [\![2]\!]^n,$$

- the cycle configuration map $C : [\![q]\!]^n \to [\![2]\!]^n$ verifying

$$C(x) = (x_{0,3n}, \ldots, x_{n-1,3n}).$$

If λ denotes either L_k or T_k or C, then for any $i \in [\![n]\!]$ and for any $x, x' \in [\![q]\!]^n$ we have $\lambda(x)_i \neq \lambda(x')_i$ implies $x_i \neq x'_i$.

Let $\sigma : [\![2]\!]^n \to [\![2]\!]^n$ be the rotation map, *i.e.* $\sigma(x)_i = x_{i+1 \bmod n}$. Let $\chi_4 = \chi_{4,n}$, $\nu_4 = \nu_{4,n}$, $\chi_2 = \chi_{2,n}$, $\nu_2 = \nu_{2,n}$. The behavior of f_Ψ consists in applying either χ_4 or the identity map on loop counters (*i.e.* incrementing or not the counter), either χ_2 or χ_2^{-1} or the identity map on truth counters (*i.e.* either incrementing, decrementing or not changing the counter) and either σ or the identity map on the cycle configuration, all choices depending on the context. Precisely $y = f_\Psi(x)$ is defined by:

1. $L_k(y) = \chi_4(L_k(x))$ if $k = n-1$ or, when $k < n-1$, if $\nu_4(L_{k+1}) = 2$ and $\nu_4(L_j(x)) = 0$ for all j, $k < j \leq n-1$. In any other case $L_k(y) = L_k(x)$.

2. We define the subformula of level k by

$$\Psi_k(x_0, \ldots, x_{k-1}) = Q_k x_k, \ldots, Q_{n-1} x_{n-1} \phi(x_0, \ldots, x_{n-1})$$

   and the Boolean value $\tau_k(x)$ which is true if and only if $\nu_4(L_k(x)) = 2$ and $\nu_4(L_j(x)) = 0$ for all j, $k < j \leq n-1$, and $\nu_2(T_k) > 0$ when $Q_k = \exists$ (resp. $\nu_2(T_k) = 2$ when $Q_k = \forall$). We say that x *raises the truth flag at level* k when $\tau_k(x)$ is true. We define the *current valuation of variable* k as $v_k(x) = \nu_4(L_k(x)) \bmod 2$ and we also define $\tau_n(x)$ as the truth of the expression $\phi(v_0(x), \ldots, v_{n-1}(x))$.

3. Then $T_k(y)$ is defined as:

   (a) $\chi_2(T_k(x))$ if $\tau_{k+1}(x)$ and $0 \leq \nu_4(L_k(x)) < 2$,

   (b) $\chi_2^{-1}(T_k(x))$ if $\tau_{k+1}(x)$ and $2 \leq \nu_4(L_k(x)) < 4$,

   (c) $\chi_2(T_k(x))$ if $4 \leq \nu_4(L_k(x)) < 4 + 2^n$ and $\nu_4(L_j(x)) = 0$ for all j, $k < j \leq n-1$,

   (d) $T_k(x)$ else.

4. we define the Boolean value $\beta(x)$ which is true if and only if for some k it holds $\nu_4(L_j(x)) = 0$ for all $j \geq k$ and $\nu_2(T_k(x)) \neq 0$. We say that the *bad counter flag is raised* if $\beta(x)$ is true.

5. Then $C(y) = \sigma(C(x))$ if either $\beta(x)$ or $\tau_0(x)$, and $C(x)$ in any other case.

The behavior of f_Ψ can be intuitively understood as follows:

1. counter L_k is incremented once during each cycle of counter L_{k+1} so that they form n nested loops that run independently of Ψ and the rest of the configuration;

2. at each level k the truth flag can be raised only at a precise moment in the cycle of the k^{th} loop counter, and if at least one valuation of variable x_k made the subformula Ψ_{k+1} "true", then the subformula Ψ_k is considered "true" when Q_k is an $\exists$ quantifier, and similarly when the two possible valuations of variable x_k made Ψ_{k+1} "true", then Ψ_k is considered "true" when $Q_k = \forall$;

3. to implement this idea, the truth counter at level k is updated according to the following cycle governed by the loop counter of level k (one step of the cycle is executed at each value change of L_k): it is incremented when the truth flag at level k+1 is raised, for each valuation of x_k during the two first steps of the cycle, then decremented when the truth flag at level $k+1$ is raised, for each valuation of x_k during the two next steps, then incremented 2^n times, then left unchanged until the end of the cycle. Concretely, if the counter started the cycle with value a then it must again be in value a at step 4 and at the first step of the next cycle, and between step 4 and $4+2^n$ it must take all possible values. The sequence of incrementations/decrementations of the counter during the cycle is independent of its initial value a;

4. a bad counter flag is raised if some truth counter was not initialized to 0 at the beginning of its cycle and therefore cannot be trusted;

5. the cycle configuration is rotated regularly if either a counter cannot be trusted or the formula Ψ is true, otherwise it is left unchanged.

Lemma 7.2. *There is an algorithm working in polynomial time that, given a quantified Boolean formula Ψ, builds circuits that compute f_Ψ (these circuits are of polynomial size).*

Proof. The construction above gives a polynomial time algorithm to build f_Ψ from Ψ, which is a collection of $3n^2 + n$ Boolean circuits which are themselves finite combinations of L_k, T_k, C, χ_q and ν_q (for $q = 2$ or 4), τ_k and β, all being circuits that can be generated in polynomial time (by Lemma 7.1 for χ_q and ν_q, and by straightforward verification for the rest). □

From the description above, the intended behavior of f_Ψ is a brute-force algorithm to test the truth of formula Ψ and make the evolution of the cycle configuration component depend on it. However this only works on well initialized configurations, while expansivity is a global property about all possible pairs of configurations. The next three lemmas show that badly initialized configurations are never a problem. First, the following lemma shows some regularity of the cycle of each counter: they always go back to their initial value after one cycle, whatever there initial value and whatever the context.

Lemma 7.3. *For any $z \in [\![q]\!]^n$ and any $k \in [\![n]\!]$, if $\nu_4(L_j(f_\Psi(z))) = 0$ for all $j \geq k$ then $T_k(f_\Psi^{4^{n(n-k)}}(z)) = T_k(z)$.*

Proof. We proceed by downward induction on k starting from $k = n-1$. For $t \in \{0,1\}$ we have that $T_{n-1}(f_\Psi^{t+1}(z)) = \chi_2(T_{n-1}(f_\Psi^t(z)))$ if and only if $T_{n-1}(f_\Psi^{t+3}(z)) = \chi_2^{-1}(T_{n-1}(f_\Psi^{t+2}(z)))$, because $v_i(f_\Psi^{t+2}(z)) = v_i(f_\Psi^t(z))$ for all $i \in [\![n]\!]$ and therefore $\tau_n(f_\Psi^{t+2}(z)) = \tau_n(f_\Psi^t(z))$. We deduce that $T_{n-1}(f_\Psi^4(z)) = T_{n-1}(z)$. We also have $T_{n-1}(f_\Psi^{4^n}(z)) = \chi_2^{2^n}(f_\Psi^4(z))$ by definition of f_Ψ. Since $\chi_2^{2^n}$ is the identity map we deduce $T_{n-1}(f_\Psi^{4^n}(z)) = T_{n-1}(z)$ which proves the induction hypothesis for $k = n-1$. Suppose now that the hypothesis holds for all levels $j \geq k+1$ ($k \leq n-2$) and consider some $z \in [\![q]\!]^n$ such that $\nu_4(L_j(f_\Psi^{t_0}(z))) = 0$ for all $j \geq k$. Denote $z_t = f_\Psi^t(z)$ for any $t \geq 0$. Let $\Delta = 4^{n(n-1-k)}$ so that $\nu_4(L_k(z_{i\cdot\Delta})) = i$ for $0 \leq i < 4^n$. By induction hypothesis and for all $k+1 \leq j < n$ we have $T_j(z_{2\Delta}) = T_j(z_0)$. We also have $L_j(z_{2\Delta}) = L_j(z_0)$ for all $k+1 \leq j < n$ and $v_j(z_{2\Delta}) = v_j(z_0)$ for all $j \in [\![n]\!]$ (because $\nu_4(L_k(z_{2\Delta})) = \nu_4(L_k(z_0)) \bmod 2$ and $L_j(z_{2\Delta}) = L_j(z_0)$ for $j \neq k$). The same equalities of counters and valuations hold between $z_{2\Delta+1}$ and z_1 because the action of f_Ψ on the counters T_j, $k+1 \leq j < n$, only depends on the values of the L_j and T_j ($k+1 \leq j < n$) and the valuations v_j for all $j \in [\![n]\!]$. By a direct induction we have the same equalities between counters of $z_{t+2\Delta}$ and z_t for $0 \leq t \leq 2\Delta$, in particular $\tau_{k+1}(z_t)$ holds if and only if $\tau_{k+1}(z_{t+2\Delta})$ holds. We deduce that $T_k(z_{t+1}) = \chi_2(T_k(z_t))$ if and only if $T_k(z_{t+\Delta+1}) = \chi_2^{-1}(T_k(z_{t+\Delta}))$ for $0 \leq t \leq 2\Delta$. It follows that $T_k(z_{4\Delta}) = T_k(z_0)$ and since $T_k(z_{4^{n(n-k)}}) = \chi_2^{2^n}(T_k(z_{4\Delta}))$ by definition of f_Ψ we finally deduce $T_k(f_\Psi^{4^{n(n-k)}}(z)) = T_k(z)$ (because $\chi_2^{2^n}$ is the identity map). □

The next two lemmas show that "bad" pairs of configurations always comply with expansivity. Given $i \in [\![n]\!]$, we say that a pair of configurations $x, x' \in [\![q]\!]^n$ is *expansive at node i* if there is $t > 0$ such that $f_\Psi^t(x)_i \neq f_\Psi^t(x')_i$.

Lemma 7.4. *If a pair of configurations x, x' differ in some loop counter (*i.e. *$L_k(x) \neq L_k(x')$ for some $k \in [\![n]\!]$) or in some truth counter (*i.e. *$T_k(x) \neq T_k(x')$ for some $k \in [\![n]\!]$) then it is expansive at node i for any $i \in [\![n]\!]$.*

Proof. Suppose first that $L_k(x) \neq L_k(x')$ for some k. By a simple downward induction on k (from $k = n-1$ to $k = 0$) and for any configuration $y \in [\![q]\!]^n$ we have $L_k(f_\Psi^{4^{n(n-1-k)}}(y)) = \chi_4(L_k(y))$. Since χ_4 is expansive (by Lemma 7.1), for any $i \in [\![n]\!]$ there is some t such that $\chi_4^t(L_k(x))_i \neq \chi_4^t(L_k(x'))_i$. We deduce that $\left(L_k(f_\Psi^{t\cdot 4^{n(n-1-k)}}(x))\right)_i \neq \left(L_k(f_\Psi^{t\cdot 4^{n(n-1-k)}}(x))\right)_i$ which means that the pair x, x' is expansive at node i. Suppose now that $L_k(x) = L_k(x')$ for all $k \in [\![n]\!]$ but $T_k(x) \neq T_k(x')$ for some k and take the largest such k. Case 3 of the definition of f_Ψ ensures for any $z \in [\![q]\!]^n$ that:

1. $T_k(f_\Psi(z)) = \lambda(T_k(z))$ where λ is either the identity, χ_2 or χ_2^{-1} and the choice of λ only depends on the values $L_j(z)$ (for $j \in [\![n]\!]$) and $T_{k+1}(z)$ (if k¡n-1).

2. if $\nu_4(L_k(z)) = 4$ and $\nu_4(L_{k+1}(z)) = 2$ (if $k < n-1$) then, for any t with $0 \leq t < 2^n$, it holds $T_k(f_\Psi^{t \cdot 4^{n(n-1-k)}}(z)) = \chi_2^t(T_k(z))$.

Now take t_0 such that $\nu_4(L_k(f_\Psi^{t_0}(x))) = \nu_4(L_k(f_\Psi^{t_0}(x'))) = 4$ (it exists because x and x' agree on all loop counters) and consider $z = f_\Psi^{t_0}(x)$ and $z' = f_\Psi^{t_0}(x')$. By point 1 above and because $T_k(x) \neq T_k(x')$ we must have $T_k(z) \neq T_k(z')$. Applying expansivity at node i of χ_2 we know there exists $0 \leq t < 2^n$ such that $\chi_2^t(T_k(z))_i \neq \chi_2^t(T_k(z'))_i$. We deduce that $T_k(f_\Psi^{t_0+t \cdot 4^{n(n-1-k)}}(x))_i \neq T_k(f_\Psi^{t_0+t \cdot 4^{n(n-1-k)}}(x'))_i$ so the pair x, x' is expansive at node i. □

Lemma 7.5. *If a pair of configurations $x \neq x'$ agrees on all counters (*i.e. *$L_k(x) = L_k(x')$ and $T_k(x) = T_k(x')$ for all k) but a bad counter flag is raised in either orbit, then this pair is expansive at any node $i \in [\![n]\!]$.*

Proof. The equality of all counters ($L_k(x) = L_k(x')$ and $T_k(x) = T_k(x')$ for all k) is preserved under iteration by definition of f_Ψ, therefore for any t it holds that $\beta(f_\Psi^t(x)) \Leftrightarrow \beta(f_\Psi^t(x'))$ and $\tau_0(f_\Psi^t(x)) \Leftrightarrow \tau_0(f_\Psi^t(x'))$. Denote by (t_n) the ordered sequence of time steps t for which either $\beta(f_\Psi^t(x))$ or $\tau_0(f_\Psi^t(x))$ holds. From the claim above we deduce that the sequence (t_n) defined above is actually infinite. Indeed, by hypothesis a bad counter flag is raised at some step t_0 in the orbit of x (equivalently of x'), which means that for some k we have $\nu_4(L_j(f_\Psi^{t_0}(x))) = 0$ for all $j \geq k$ and $\nu_2(T_k(f_\Psi^{t_0}(x))) \neq 0$. The claim implies that $\nu_2(T_k(f_\Psi^{t_0+m \cdot 4^{n(n-k)}}(x))) \neq 0$ for any $m \geq 0$ (note that $m \cdot 4^{n(n-k)}$ is a multiple of the period of all counters L_j for $j \geq k$). The sequence (t_n) is such that for any $n \geq 0$ we have both $C(f_\Psi^{1+t_n}(x)) = \sigma^n(C(x))$ and $C(f_\Psi^{1+t_n}(x')) = \sigma^n(C(x'))$. Finally, consider $j \in [\![n]\!]$ such that $C(x)_j \neq C(x')_j$ and any $i \in [\![n]\!]$, so that $\sigma^{i-j \bmod n}(C(x))_i \neq \sigma^{i-j \bmod n}(C(x'))_i$. We deduce that $f_\Psi^{1+t_{i-j \bmod n}}(x)_i \neq f_\Psi^{1+t_{i-j \bmod n}}(x')_i$. □

The next lemma shows the link between the truth of Ψ and the behavior of f_Ψ on "good" pairs of configuration.

Lemma 7.6. *If a pair of configuration $x \neq x'$ agrees on all counters and no bad counter flag is raised in their orbits, then the pair is expansive if the formula Ψ is true. Moreover, if Ψ is false and $x_i = x'_i$ for some $i \in [\![n]\!]$ then the pair is not expansive at node i.*

Proof. First, as said in the proof of Lemma 7.5, equality of counters is preserved under iteration and therefore predicate τ_0 is true at step t in the orbit of x if and only if τ_0 is true at step t in the orbit of x'. This implies that for all t there is t' such that $C(f_\Psi^t(x)) = \sigma^{t'}(C(x))$ and $C(f_\Psi^t(x')) = \sigma^{t'}(C(x'))$ and in particular it is always the case that $C(f_\Psi^t(x)) \neq C(f_\Psi^t(x'))$. So we can suppose without loss of generality that $\nu_4(L_k(x)) = \nu_4(L_k(x')) = 0$ for all $k \in [\![n]\!]$ (otherwise we consider configurations at the same time step in both orbits for which it is the case). We must also have $\nu_2(T_k(x)) = \nu_2(T_k(x')) = 0$ for all $k \in [\![n]\!]$ because no bad counter flag is raised by hypothesis. We show by downward induction on k starting from $k = n-1$ that for any y in the orbit

of x such that $\nu_4(L_k(y)) = 2$ and $\nu_4(L_j(y)) = 0$ for all $k < j \leq n-1$, then $\tau_k(y)$ holds if and only if $\Psi_k(v_0(y), \ldots, v_{k-1}(y))$ is true. Take any configuration $y = f_\Psi^t(x)$ in the orbit of x with $\nu_4(L_{n-1}(y)) = 2$, and let $y^{-1} = f_\Psi^{t-1}(x)$ and $y^{-2} = f_\Psi^{t-2}(x)$ (t must be greater than 2 because $\nu_4(L_{n-1}(x)) = 0$ by hypothesis). We have $\nu_4(L_{n-1}(y^{-2})) = 0$ and $\nu_2(T_{n-1}(y^{-2})) = 0$ (no bad counter flag hypothesis). Therefore $\nu_2(T_{n-1}(y^{-1})) = 1$ if and only if τ_n is true, *i.e.* if $\phi(v_0(y^{-2}), \ldots, v_{n-1}(y^{-2}))$ is true. Similarly $\nu_2(T_{n-1}(y)) = \nu_2(T_{n-1}(y^{-1})) + \delta$ where $\delta = 1$ is $\phi(v_0(y^{-1}), \ldots, v_{n-1}(y^{-1}))$ is true and 0 otherwise. Said differently, since $v_{n-1}(y^{-2}) = 0$ and $v_{n-1}(y^{-2}) = 1$ and $v_j(y^{-2}) = v_j(y^{-1})$ for $0 \leq j < n-1$, $\nu_2(T_{n-1}(y)) = \#\{v \in \{0,1\} : \phi(v_0(y), \ldots, v_{n-1}(y))\}$. Thus, $\tau_{n-1}(y)$ is true if and only if $\#\{v \in \{0,1\} : \phi(v_0(y), \ldots, v_{n-1}(y))\} \geq 1$ when $Q_{n-1} = \exists$ and if and only if $\#\{v \in \{0,1\} : \phi(v_0(y), \ldots, v_{n-1}(y))\} = 2$ when $Q_{n-1} = \forall$. This exactly means that $\tau_{n-1}(y)$. The induction step is similar and hence omitted. We have shown in particular that if y verifies $\nu_4(L_0(y)) = 2$ and $\nu_4(L_j(y)) = 0$ for all $0 < j \leq n-1$, then $\tau_0(y)$ holds if and only if $\Psi_0 = \Psi$ is true. We deduce that if Ψ is false then $C(y) = C(x)$ for any y in the orbit of x, and therefore if the pair x, x' is such that $C(x) \neq C(x')$ but $C(x)_i = C(x')_i$, then it is not expansive at node i. On the contrary, if Ψ is true, then for any t' there is t such that $C(f_\Psi^t(x)) = \sigma^{t'}(C(x))$ so any pair satisfying the hypothesis of the lemma is expansive at any node. □

Theorem 7.7. *Problem EXPAN is PSPACE-complete.*

Proof. It is straightforward to check expansivity in polynomial space (for each node and each pair of configurations test if their orbits differ at the node at some time step bounded by q^n where n is the size of the network and q the state set). PSPACE-hardness follows from the lemmas and the fact that deciding whether a quantified Boolean formula is true is a PSPACE-complete problem. □

Note that our construction actually shows that it is PSPACE-complete to separate networks which are expansive (the trace ρ_v is injective for any node v) from networks which are not expansive at any single node (for all v, the trace ρ_v is not injective). It also shows that it is PSPACE-complete to decide whether a network is quasi-expansive because the constructed network is either expansive, or acts as the identity on the cycle configuration and thus cannot be quasi-expansive. Moreover, our result actually improves the co-NP-hardness of observability proven in [11] because, as said in the introduction, expansivity can be seen as a particular form of observability (where the output of the system is the trace at some node). Finally, the alphabet size in our construction only depend on the number of quantifiers in the formula, so we actually show Σ_p-hardness for each level p of the polynomial hierarchy with a fixed alphabet size.

8. Stronger form of expansivity

The notion of expansivity considered so far asks to determine the initial configuration from the trace at any given node. Here, we strengthen the notion by

asking to determine the initial configuration from any large enough 'observation' of the network during the first n time steps. Let $f \in \mathrm{F}(n,q)$. Consider any sequence ω of n pairs (vertex, time step): $\omega = \big((v_1,t_1),\dots,(v_n,t_n)\big)$ where $v_i \in [\![n]\!]$ and $t_i \in [\![n]\!]$ for all i such that $1 \le i \le n$. The associated *observation* is the map $\tau_\omega : [\![q]\!]^n \to [\![q]\!]^n$ given by $\tau_\omega(x) = \big(f^{t_1}(x)_{v_1}, f^{t_2}(x)_{v_2}, \dots, f^{t_n}(x)_{v_n}\big)$. We say f is **super-expansive** if for any ω, the map τ_ω is injective. Looking again at matrix M_x defined previously, f is super-expansive if x can be determined from any set of n entries in this matrix.

Proposition 8.1. *Let D be a graph with n nodes. If $f \in \mathrm{F}[D,q]$ is super-expansive, then D is the complete graph (the graph with n^2 arcs).*

Proof. Suppose that D does not contain the arc ij and consider any $f \in \mathrm{F}[D,q]$. Let $\omega = \big((1,1),\dots,(i-1,1),(j,2),(i+1,1),\dots,(n,1)\big)$, then the interaction graph of τ_ω has a source (namely i) and hence is not coverable. Thus, by [5, Corollary 6], τ_ω is not bijective. □

Using a similar technique as in the proof of Theorem 3.10 we can show the existence of super-expansive networks.

Theorem 8.2. *For any n and any prime power $q > n^2\binom{n^2}{n}$ there exists a super-expansive linear network with n nodes over* $\mathrm{GF}(q)$.

Proof. The proof technique is similar to that of Theorem 3.10. First for any linear function $f(x) = xM$ and any $\omega = \big((v_1,t_1),\dots,(v_n,t_n)\big)$, the observation τ_ω is injective if and only if the matrix

$$N_\omega := \left(\begin{array}{c|c|c|c} M_{v_1}^{t_1} & M_{v_2}^{t_2} & \dots & M_{v_n}^{t_n} \end{array} \right)$$

is nonsingular (straightforward adaptation of Lemma 2.2). Since injectivity of τ_ω is preserved by permutation of ω, we suppose that $t_1 \le t_2 \le \dots \le t_n$. Like for Theorem 3.10 our proof is nonconstructive: we shall see the nonzero coefficients of the matrix M as variables $(X_{ij})_{i,j\in[\![n]\!]}$, then the determinant of N_ω is a polynomial of these variables; if the field is large enough, then we can always evaluate that polynomial to something other than zero, provided it is not the null polynomial. Using the correspondence between walks on the complete graph and monomials, the determinant of N_ω can be expressed as:

$$\det(N_\omega) = \sum_{\sigma\in S_n} \epsilon(\sigma) P_\sigma$$

where each monomial appearing in P_σ is of the form $\prod_{i=1}^n \prod_{k=1}^{t_i} X_{w_i(k)}$ where $w_i(1)\cdots w_i(t_i)$ is a walk of length t_i from node $\sigma(i)$ to node v_i. We shall now choose a specific permutation σ and a specific monomial appearing in P_σ, and show that it does not appear in any other $P_{\sigma'}$ for $\sigma \neq \sigma'$. Let $A = \{v_1,\dots,v_n\}$ and choose $v'_1,\dots,v'_n$ distinct nodes verifying:

$$v'_i = \begin{cases} v_i & \text{if } i = \min\{k : v_i = v_k\} \\ \notin A & \text{else.} \end{cases}$$

Our permutation is $\sigma = i \mapsto v'_i$, and we consider the monomial $M = \prod_i X_{v'_i v'_i}^{t_i - 1} X_{v'_i v_i}$ which clearly appears in P_σ. Consider any permutation σ' and suppose that M appears in $P_{\sigma'}$, *i.e.* $M = \prod_{i=1}^{n} \prod_{k=1}^{t_i} X_{w_i(k)}$ where $w_i(1) \cdots w_i(t_i)$ is a walk of length t_i from node $\sigma'(i)$ to node v_i. For each $v \in A$, let $I_v = \{i : v_i = v\}$. If $I_v = \{i\}$ is a singleton then we must have $\sigma(i) = v_i$ because in this case no other edge than $v_i v_i$ arrives at v_i and appears in M. If not, let $k = \max I_v$. Since $v'_k \notin A$ and since in M there is no edge arriving at v'_k other that $v'_k v'_k$ and no edge starting from v'_k other than $v'_k v_i$, then the only walk that can contain edge $v'_k v'_k$ is a walk starting from v'_k, arriving at v and it must be of length t_k to exhaust the power of $X_{v'_k v'_k}$ in M. Therefore, we must have $\sigma'(k) = v'_k$. Continuing with the same reasoning we show that σ and σ' are equal on I_v for all v, which means $\sigma' = \sigma$. This shows that $\det(N_\omega) \neq 0$.

The degree of N_ω is clearly at most n^2. By the Schwartz-Zippel Lemma [23, Theorem 7.1.4], there are at most $n^2 q^{n^2-1}$ choices for the values of X_e for which $\det(N_\omega) = 0$. Thus, there are at most $n^2 \binom{n^2}{n} q^{n^2-1}$ choices for the values of X_e for which some observation τ_ω fails to be injective (recall that injectivity of τ_ω is preserved by permutation of ω). Since $q > n^2 \binom{n^2}{n}$, we have $q^{n^2} > n^2 \binom{n^2}{n} q^{n^2-1}$, and hence there exists a choice of values for all the variables X_e such that M is super-expansive. □

As an application, we shall see that any super-expansive (linear) network naturally gives rise to a (linear) orthogonal array and a maximum distance separable code. This can be formalized as follows (see [12, 13] for an overview of the topic).

An *orthogonal array* of strength s over alphabet $[\![q]\!]$ and of index 1 is a $N \times M$ array $\mathcal{A}$ of elements of $[\![q]\!]$ with $s \leq N$ and such that for any set of s columns of $\mathcal{A}$ no s-tuple appears two times. When q is a prime power, we say the orthogonal array $\mathcal{A}$ is linear if the set of rows is a vector space over $\mathrm{GF}(q)$. A code $\mathcal{C}$ is a set of words from $[\![q]\!]^N$ and its minimal distance $d(\mathcal{C})$ is the minimal Hamming distance between two distinct elements of $\mathcal{C}$. When q is a prime power, a code $\mathcal{C}$ is linear if it forms a sub-vector space of $\mathrm{GF}(q)^N$. A maximum distance separable (MDS) code is a code verifying the equality in the so-called Singleton bound [13], *i.e.* such that $|\mathcal{C}| = q^{N - d(\mathcal{C}) + 1}$.

The link between these combinatorial objects and super-expansive networks is as follows. Given any $f \in \mathrm{F}(n, q)$ let $\mathcal{A}_f$ be the $n^2 \times q^n$ array whose set of rows is $\{L_x : x \in [\![q]\!]^n\}$ where

$$L_x = (f(x)_1, f(x)_2, \ldots, f(x)_n, f^2(x)_1, \ldots, f^2(x)_n, \ldots, f^n(x)_1, \ldots, f^n(x)_n).$$

Proposition 8.3. *If $f \in \mathrm{F}(n, q)$ is super-expansive then $\mathcal{A}_f$ is an orthogonal array of strength n and index 1, and its set of rows is an MDS code of minimum distance $n^2 - n + 1$. If moreover q is a prime power and f is linear, then $\mathcal{A}_f$ is linear and its set of rows is an MDS linear code.*

Proof. To any set of n columns of $\mathcal{A}_f$ is naturally associated $\omega = (v_1, t_1), \ldots, (v_n, t_n)$. The fact that τ_ω is injective (by super-expansivity of f) exactly means that no

pair of distinct lines L_x can coincide on this set of columns. Hence, $\mathcal{A}_f$ is an orthogonal array of strength n. The fact that it also correspond to a MDS code is well-known and general [12, Theorem 4.21]. Finally, it is straightforward to see that when f is linear then $\mathcal{A}_f$ is a linear and the corresponding code also. □

Using the classical bound of K. A. Bush on MDS codes [26], we get a lower bound on the alphabet of a super-expansive network.

Corollary 8.4. *There is no super-expansive network with n nodes over the alphabet $[\![q]\!]$ if $q \leq n^2 - n$.*

Proof. This follows immediately from the Bush bound [26], which states that any orthogonal array of index 1, strength t over alphabet $[\![q]\!]$ of size $N \times M$ verifies: $N \leq t + q - 1$. The corollary follows from the previous proposition with $N = n^2$ and $t = n$. □

9. Perspectives

The results presented above leave us with a contrasted global picture: on one hand, expansivity is easy to characterize and ubiquitous on linear systems as soon as simple graph theoretical constraints on the network are satisfied, and, on the other hand, the general (non-linear) case provides behaviors that are impossible in the linear case (e.g. exponential expansion time) but is PSPACE-hard to decide. Among the possible future research directions, we would like to put forward the following:

- When making the parallel with cellular automata, it is striking that we obtained a hardness result for expansivity in automata networks, while decidability of positive expansivity in cellular automata is still a major open problem (see [20, Problem 19] or [21, Problem 7]). To that extent, we think that two restrictions on the possible inputs of the EXPAN problem are important to study: bounded degree networks and uniformity of the local rules (like in cellular automata).

- Several results above gave some hints on the crucial role of the alphabet. We are far from understanding to property of expansivity for fixed alphabet, starting from the characterization of their of interaction graph. In particular, we left open this simple question: do strongly connected and coverable graphs of degree d admit expansive networks of alphabet bounded by d?

- Beyond expansivity, we think that many classical properties of topological dynamics [8] can be adapted to automata networks through the notion of trace which is central in this paper. For instance, one can imagine meaningful notions of mixingness, transitivity or equicontinuity points for automata networks, and study there relations to expansivity. We also think that studying the traces of automata networks from a formal language point of view is promising.

10. References

References

[1] M. Gadouleau, A. Richard, Simple dynamics on graphs, Theoretical Computer Science 628 (2016) 62–77.

[2] A. Wu, A. Rosenfeld, Cellular graph automata. i. basic concepts, graph property measurement, closure properties, Information and Control 42 (3) (1979) 305 – 329. doi:https://doi.org/10.1016/S0019-9958(79)90288-2.
URL http://www.sciencedirect.com/science/article/pii/S0019995879902882

[3] A. Wu, A. Rosenfeld, Cellular graph automata. ii. graph and subgraph isomorphism, graph structure recognition, Information and Control 42 (1979) 330–353. doi:10.1016/S0019-9958(79)90296-1.

[4] M. Gadouleau, On the influence of the interaction graph on a finite dynamical system, Natural Computing.
URL https://arxiv.org/abs/1805.12247

[5] M. Gadouleau, On the rank and periodic rank of finite dynamical systems, The Electronic Journal of Combinatorics 25 (3) (2018) 1–16.

[6] M. Gadouleau, S. Riis, Graph-theoretical constructions for graph entropy and network coding based communications, IEEE Transactions on Information Theory 57 (10) (2011) 6703–6717.

[7] W. R. Utz, Unstable homeomorphisms, Proceedings of the American Mathematical Society 1 (6) (1950) 769–774.
URL http://www.jstor.org/stable/2031982

[8] P. Kůrka, Topological and symbolic dynamics, Société Mathématique de France, 2003.

[9] M. Boyle, D. Lind, Expansive subdynamics 349 (1) (1997) 55–102.
URL http://www.math.umd.edu/~mmb/papers/subdynamics.pdf

[10] P. Collins, J. van Schuppen, Observability of hybrid systems and turing machines, in: 2004 43rd IEEE Conference on Decision and Control (CDC) (IEEE Cat. No.04CH37601), IEEE, 2004. doi:10.1109/cdc.2004.1428598.
URL https://doi.org/10.1109/cdc.2004.1428598

[11] D. Laschov, M. Margaliot, G. Even, Observability of boolean networks: A graph-theoretic approach, Automatica 49 (8) (2013) 2351–2362. doi:10.1016/j.automatica.2013.04.038.
URL https://doi.org/10.1016/j.automatica.2013.04.038

[12] A. Hedayat, N. Sloane, J. Stufken, Orthogonal Arrays, Springer-Verlag, New York, 1999.

[13] F. J. MacWilliams, N. J. A. Sloane, The Theory of Error-Correcting Codes, North-Holland, Amsterdam, 1977.

[14] J. Bang-Jensen, G. Gutin, Digraphs: Theory, Algorithms and Applications, Springer, 2009.

[15] A. V. Aho, J. E. Hopcroft, J. D. Ullman, The Design and Analysis of Computer Algorithms, Addison-Wesley, 1974.

[16] F. Blanchard, A. Maass, Dynamical properties of expansive one-sided cellular automata, Israel Journal of Mathematics 99 (1997) 149–174.

[17] M. Pivato, Positive expansiveness versus network dimension in symbolic dynamical systems, Theor. Comput. Sci. 412 (30) (2011) 3838–3855. doi:10.1016/j.tcs.2011.02.021.

[18] M. Nasu, Nondegenerate q-biresolving textile systems and expansive cellular automata of onesided full shifts, Transactions of the American Mathematical Society 358 (2006) 871–891.

[19] J. Jalonen, J. Kari, On dynamical complexity of surjective ultimately right-expansive cellular automata, in: Cellular Automata and Discrete Complex Systems - 24th IFIP WG 1.5 International Workshop, AUTOMATA 2018, Ghent, Belgium, June 20-22, 2018, Proceedings, 2018, pp. 57–71. doi:10.1007/978-3-319-92675-9_5.
URL https://doi.org/10.1007/978-3-319-92675-9_5

[20] M. Boyle, Open problems in symbolic dynamics, Contemporary Mathematics 469 (2008) 69–118.

[21] J. Kari, Theory of cellular automata: A survey, Theoretical Computer Science 334.

[22] J. Edmonds, Systems of distinct representatives and linear algebra, Journal of Research of the National Bureau of Standards B 71B (1967) 241–245.

[23] G. L. Mullen, D. Panario, Handbook of Finite Fields, CRC Press, 2013.

[24] E. R. Berlekamp, Algebraic Coding Theory, McGraw-Hill, 1968.

[25] L. J. Stockmeyer, A. R. Meyer, Word problems requiring exponential time(preliminary report), in: Proceedings of the Fifth Annual ACM Symposium on Theory of Computing, STOC '73, ACM, New York, NY, USA, 1973, pp. 1–9. doi:10.1145/800125.804029.
URL http://doi.acm.org/10.1145/800125.804029

[26] K. A. Bush, Orthogonal arrays of index unity, Ann. Math. Statist. 23 (3) (1952) 426–434. doi:10.1214/aoms/1177729387.
URL https://doi.org/10.1214/aoms/1177729387